# งานนี้เป็นส่วนหนึ่งของ **LAB 2: Windows Security Hardening**

**โดยผู้จัด นายพัสกร บทศรี ทำรับผิดชอบ Task 1–3**

**ส่วน นาย ธนพล ผายาว  รับผิดชอบ Task4-5**

บน Windows Server 2019 (VM – VirtualBox) เพื่อเพิ่มความปลอดภัยด้านบัญชีผู้ใช้ นโยบายรหัสผ่าน/ล็อกเอาต์ และการป้องกันมัลแวร์/ไฟร์วอลล์

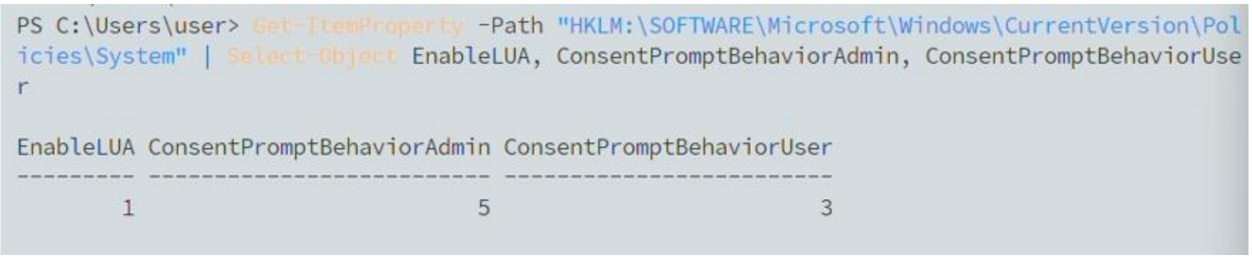
## Task 1 – Configure User Account Control (UAC) & Users

**วัตถุประสงค์:**
 กำหนดระดับ UAC ให้เข้มงวดที่สุดและแยกบทบาทผู้ใช้เป็น Dev/Test/Admin

**สภาพแวดล้อม:** PowerShell (Run as Administrator)

**ขั้นตอนที่ทำ:**

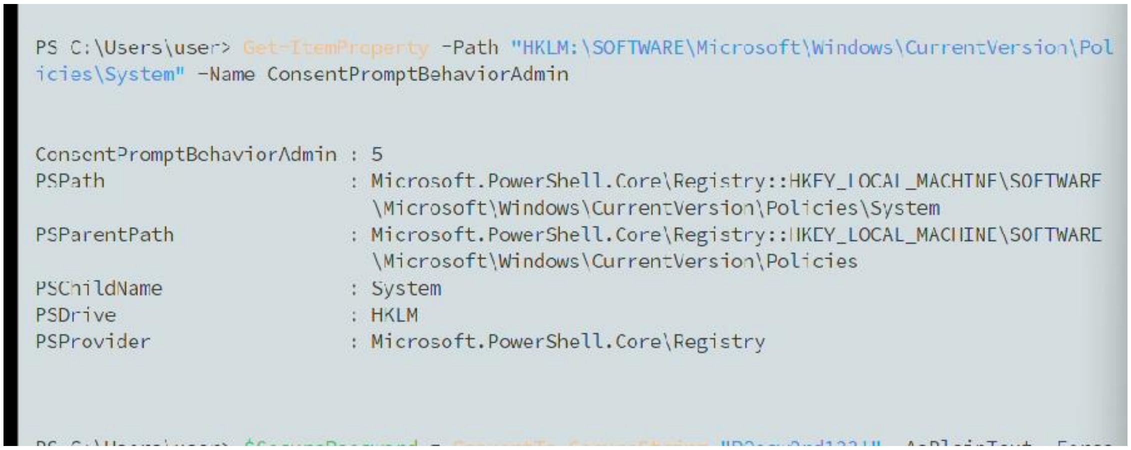
1. ตรวจสอบค่า UAC ปัจจุบัน



```
PS C:\Users\user> Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" | Select-Object EnableLUA, ConsentPromptBehaviorAdmin, ConsentPromptBehaviorUse
r

EnableLUA ConsentPromptBehaviorAdmin ConsentPromptBehaviorUser
--------- -------------------------- -------------------------
        1                          5                         3
```

จะแสดงค่าเริ่มต้นของ UAC Settings เช่น:

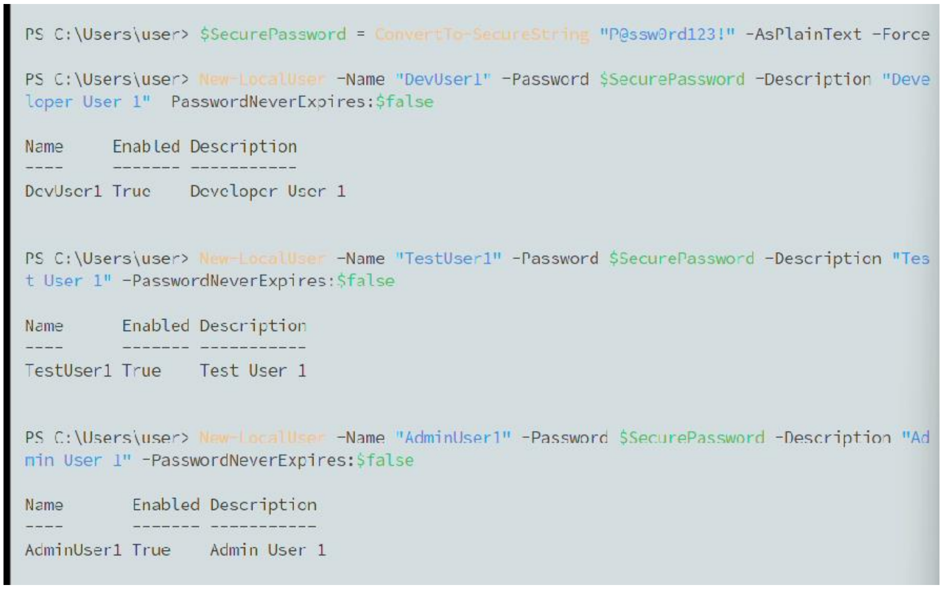
- EnableLUA: 1 (เปิดใช้งาน UAC) หรือ 0 (ปิดใช้งาน)
- ConsentPromptBehaviorAdmin: 0-2 (ระดับการยืนยันสำหรับผู้ดูแล)
- ConsentPromptBehaviorUser: 0-3 (ระดับการยืนยันสำหรับผู้ใช้ทั่วไป)



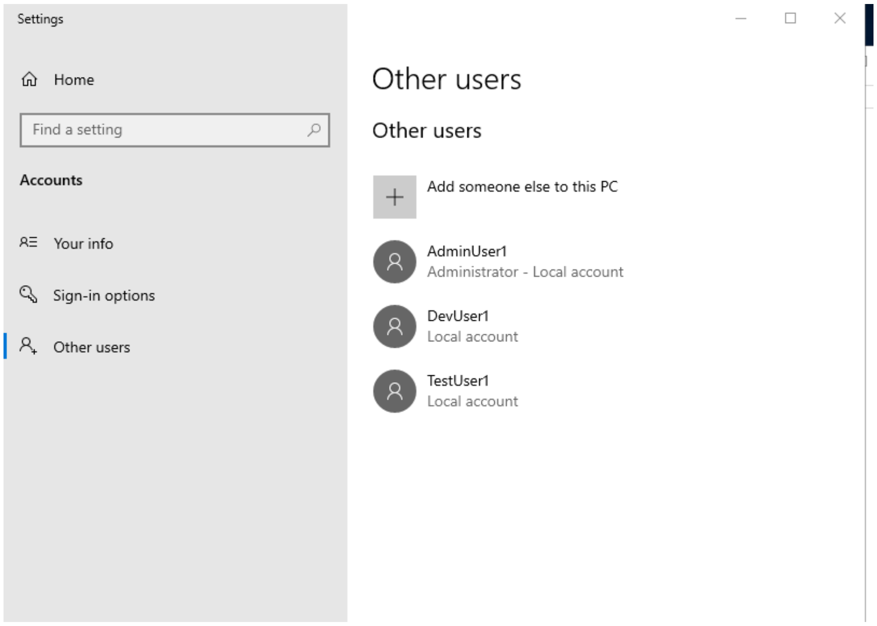
```
PS C:\Users\user> Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" -Name ConsentPromptBehaviorAdmin


ConsentPromptBehaviorAdmin : 5
PSPath                     : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
                             \Microsoft\Windows\CurrentVersion\Policies\System
PSParentPath               : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
                             \Microsoft\Windows\CurrentVersion\Policies
PSChildName                : System
PSDrive                    : HKLM
PSProvider                 : Microsoft.PowerShell.Core\Registry



PS C:\Users\user> $SecurePassword = ConvertTo-SecureString "P@ssw0rd123!" -AsPlainText -Force
```

สร้างผู้ใช้และกำหนดกลุ่ม

- สร้าง DevUser1, TestUser1, AdminUser1 ด้วยรหัสผ่านตามนโยบาย
- เพิ่ม DevUser1, TestUser1 เข้า **Users** และเพิ่ม AdminUser1 เข้า **Administrators**
- สร้างผู้ใช้ 3 ราย: DevUser1, TestUser1, AdminUser1
- DevUser1 และ TestUser1 อยู่ในกลุ่ม Users
- AdminUser1 อยู่ในกลุ่ม Administrators
- ผลลัพธ์จาก Get-LocalUser จะแสดงรายละเอียดผู้ใช้ เช่น Name, Enabled, PasswordExpire



```
PS C:\Users\user> $SecurePassword = ConvertTo-SecureString "P@ssw0rd123!" -AsPlainText -Force

PS C:\Users\user> New-LocalUser -Name "DevUser1" -Password $SecurePassword -Description "Deve
loper User 1"  PasswordNeverExpires:$false

Name     Enabled Description
----     ------- -----------
DevUser1 True    Developer User 1


PS C:\Users\user> New-LocalUser -Name "TestUser1" -Password $SecurePassword -Description "Tes
t User 1" -PasswordNeverExpires:$false

Name      Enabled Description
----      ------- -----------
TestUser1 True    Test User 1


PS C:\Users\user> New-LocalUser -Name "AdminUser1" -Password $SecurePassword -Description "Ad
min User 1" -PasswordNeverExpires:$false

Name       Enabled Description
----       ------- -----------
AdminUser1 True    Admin User 1
```



Settings

Home

Find a setting

Accounts

Your info

Sign-in options

Other users

Other users

Other users

Add someone else to this PC

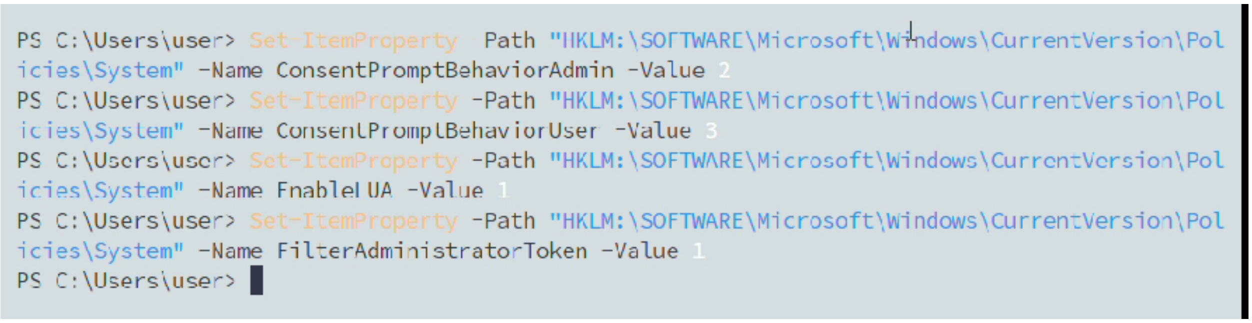
AdminUser1
Administrator - Local account

DevUser1
Local account

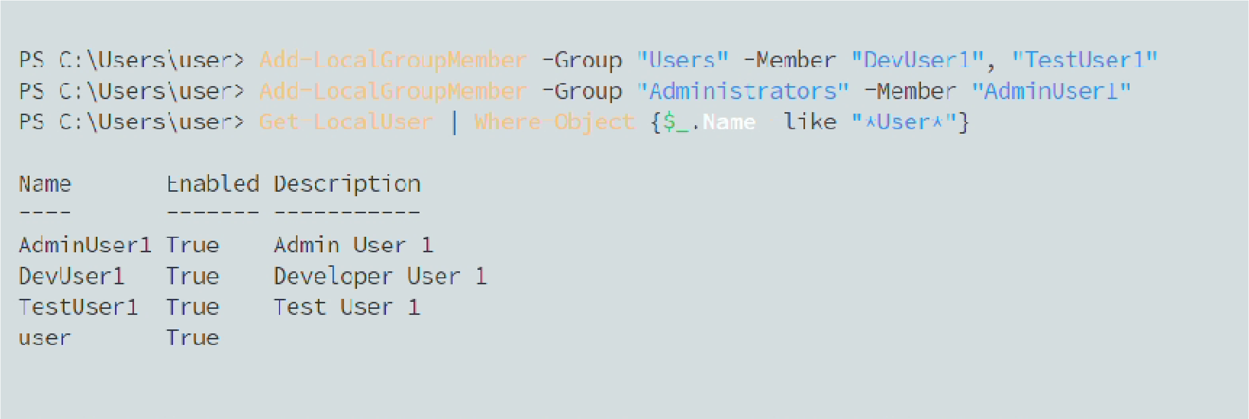
TestUser1
Local account

ปรับระดับ UAC

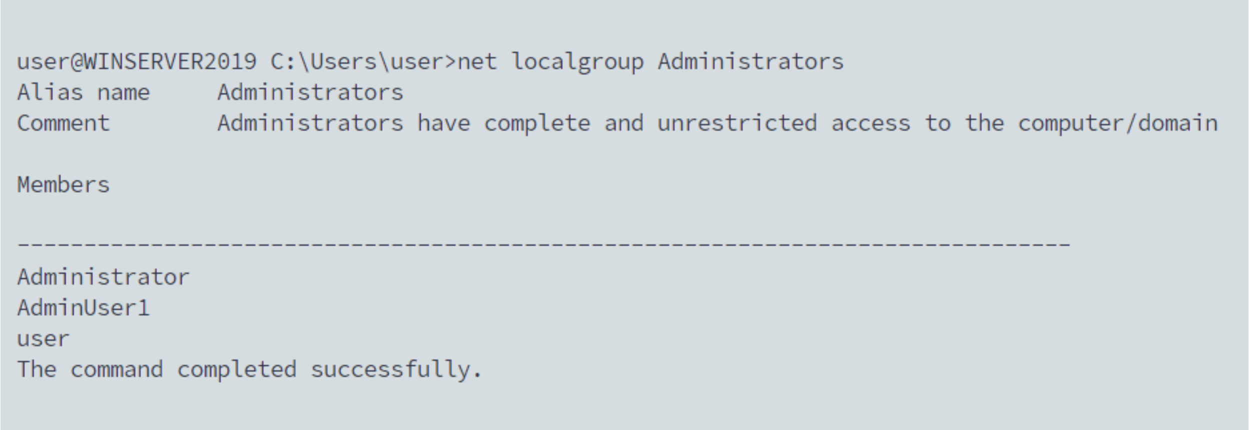
- ConsentPromptBehaviorAdmin = 2: ผู้ดูแลต้องยืนยันทุกการกระทำที่ต้องการสิทธิ์สูง
- ConsentPromptBehaviorUser = 3: ผู้ใช้ทั่วไปถูกบล็อกจากการรันโปรแกรมที่ต้องการสิทธิ์สูง
- EnableLUA = 1: เปิดใช้งาน UAC
- FilterAdministratorToken = 1: เปิดโหมด Admin Approval Mode



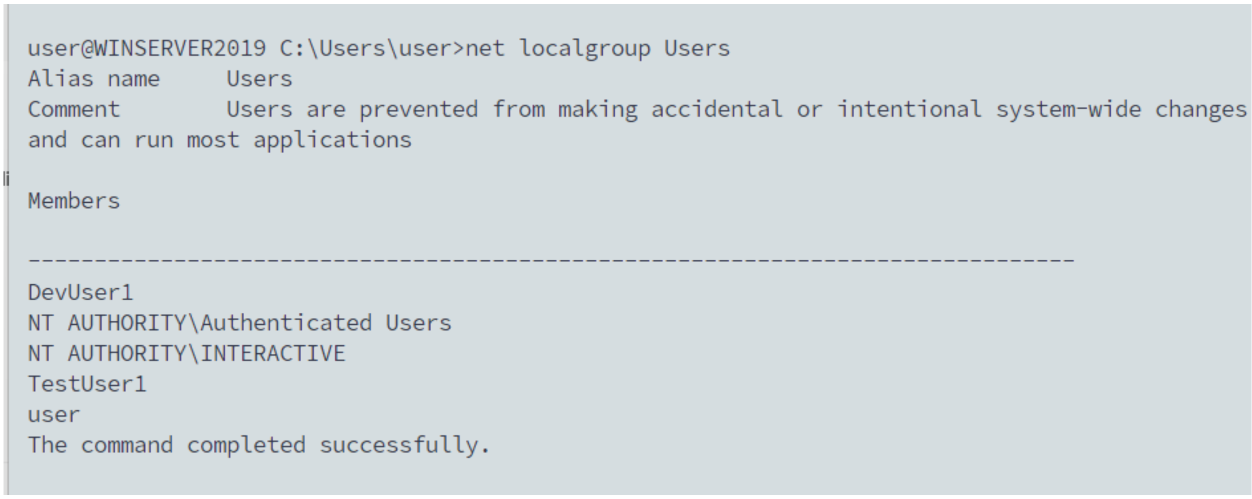
```
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" -Name ConsentPromptBehaviorAdmin -Value 2
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" -Name ConsentPromptBehaviorUser -Value 3
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" -Name EnableLUA -Value 1
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" -Name FilterAdministratorToken -Value 1
PS C:\Users\user>
```



```
PS C:\Users\user> Add-LocalGroupMember -Group "Users" -Member "DevUser1", "TestUser1"
PS C:\Users\user> Add-LocalGroupMember -Group "Administrators" -Member "AdminUser1"
PS C:\Users\user> Get-LocalUser | Where-Object {$_.Name -like "*User*"}

Name       Enabled Description
----       ------- -----------
AdminUser1 True    Admin User 1
DevUser1   True    Developer User 1
TestUser1  True    Test User 1
user       True
```



```
user@WINSERVER2019 C:\Users\user>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
AdminUser1
user
The command completed successfully.
```

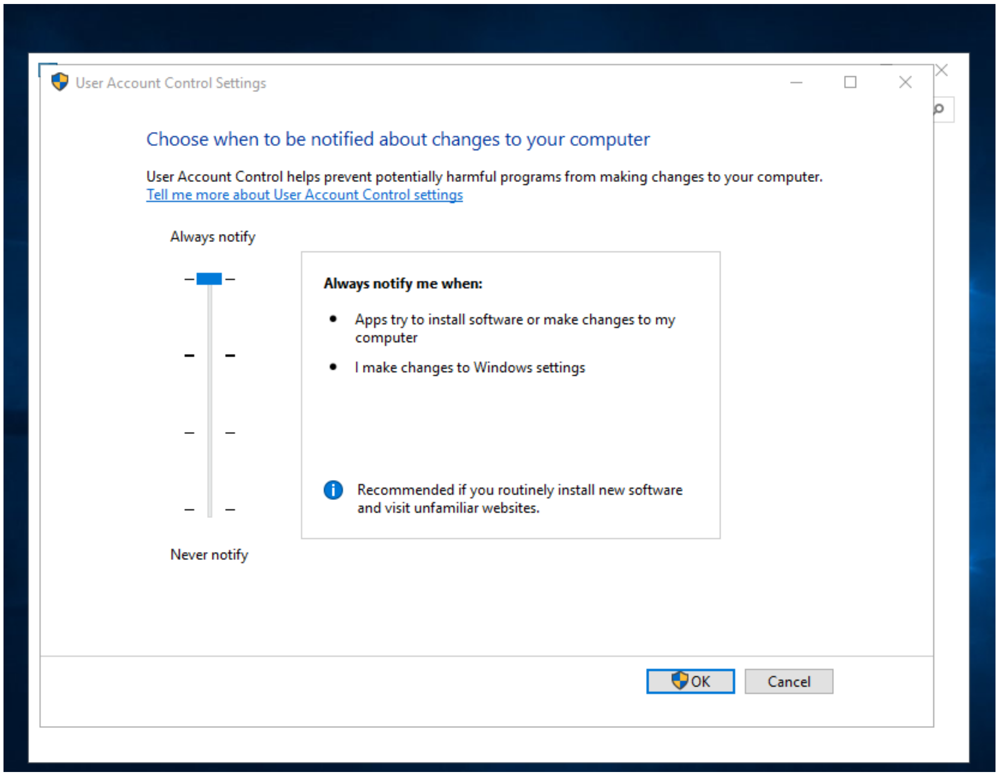


```
user@WINSERVER2019 C:\Users\user>net localgroup Users
Alias name     Users
Comment        Users are prevented from making accidental or intentional system-wide changes
and can run most applications

Members

-------------------------------------------------------------------------------
DevUser1
NT AUTHORITY\Authenticated Users
NT AUTHORITY\INTERACTIVE
TestUser1
user
The command completed successfully.
```

ตรวจสอบ **UAC Control Panel Settings**:

- ไปที่ **Control Panel > User Accounts > Change User Account Control settings**

- ปรับสไลเดอร์ไปที่ **Always notify** (ระดับสูงสุด) เพื่อให้สอดคล้องกับการตั้งค่า ConsentPromptBehaviorAdmin = 2



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

**Always notify me when:**

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

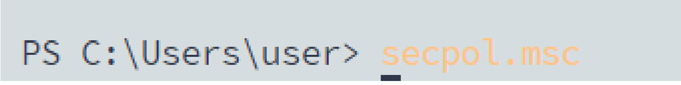
Recommended if you routinely install new software and visit unfamiliar websites.

Never notify

## Task 2: Set up Group Policy

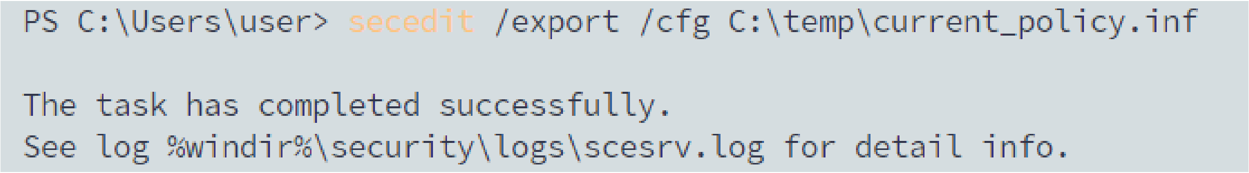
2.1 Configure Local Security Policy:

เปิด Local Security Policy



```
PS C:\Users\user> secpol.msc
```

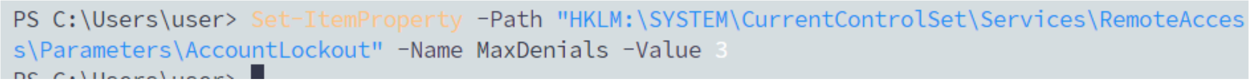
ตรวจสอบไฟล์ current_policy.inf ในโฟลเดอร์ C:\temp



```
PS C:\Users\user> secedit /export /cfg C:\temp\current_policy.inf

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
```

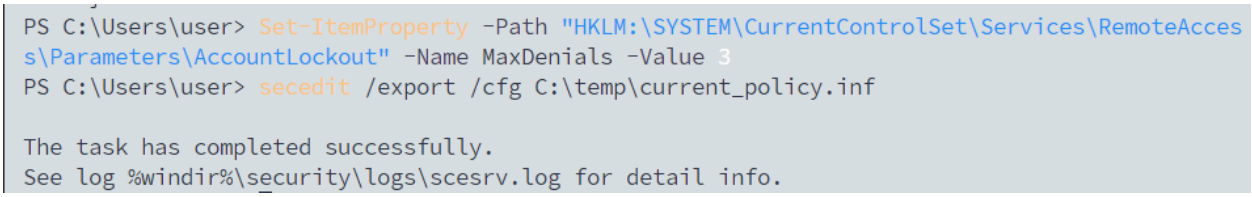
ปรับแต่ง Account Lockout Policy ผ่าน Registry

ค่า MaxDenials = 3 กำหนดให้ล็อกบัญชีหลังพยายามล็อกอินผิด 3 ครั้ง



```
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\RemoteAcces
s\Parameters\AccountLockout" -Name MaxDenials -Value 3
PS C:\Users\user>
```

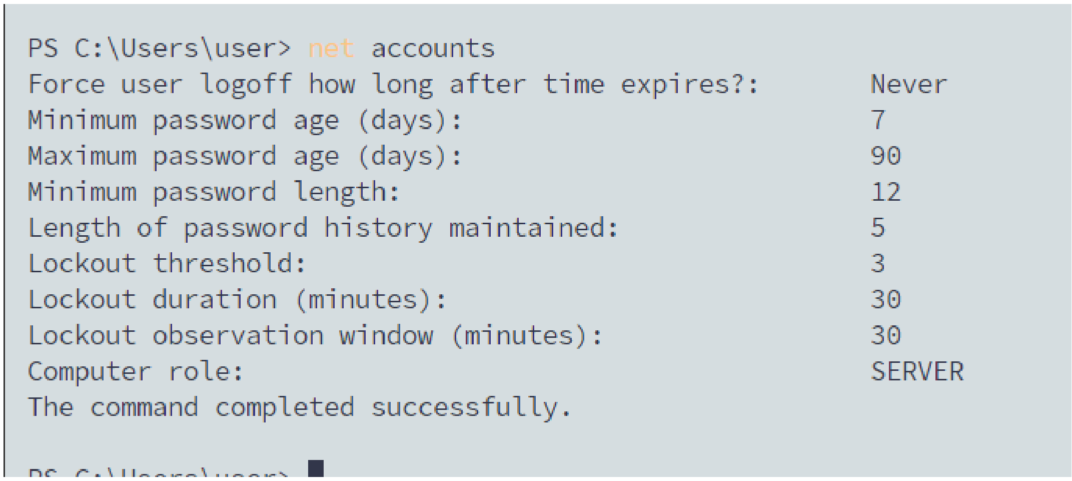
ตรวจสอบไฟล์ current_policy.inf ใน C:\temp เพื่อดูนโยบาย



```
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\RemoteAcces
s\Parameters\AccountLockout" -Name MaxDenials -Value 3
PS C:\Users\user> secedit /export /cfg C:\temp\current_policy.inf

The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
```

## 2.2 Password Policy Configuration:

สร้างไฟล์ Batch เพื่อกำหนดนโยบายรหัสผ่าน

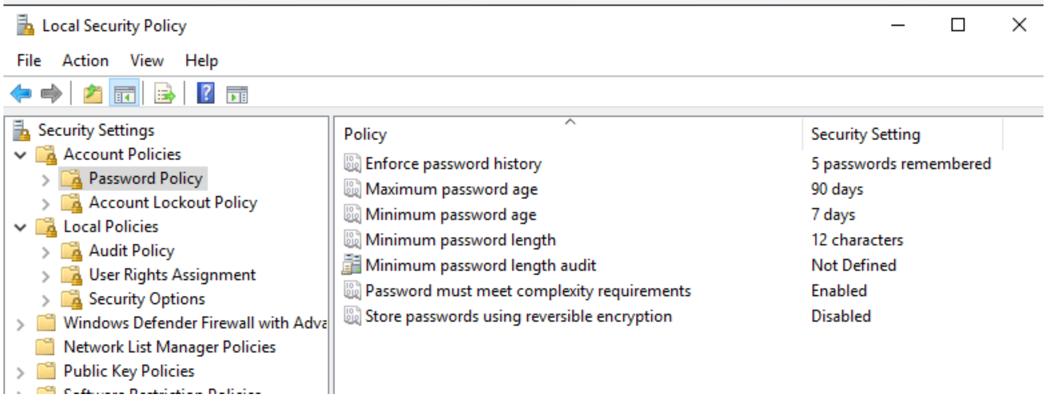


```
PS C:\Users\user> net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          7
Maximum password age (days):                          90
Minimum password length:                              12
Length of password history maintained:                5
Lockout threshold:                                    3
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        SERVER
The command completed successfully.

PS C:\Users\user>
```

ความหมาย: รหัสผ่านต้องยาว 12 ตัวอักษร, เปลี่ยนได้หลัง 7 วัน, หมดอายุ 90 วัน, ต้องซับซ้อน, จำกัดประวัติ 5 รหัส, ล็อก 30 นาทีหลังผิด 3 ครั้ง

```
secedit /configure /db C:\temp\secedit.sdb /cfg C:\temp\password_policy.inf
```

ผลลัพธ์นี้ยืนยันว่านโยบายรหัสผ่านถูกปรับตามข้อกำหนดเพื่อเพิ่มความปลอดภัย



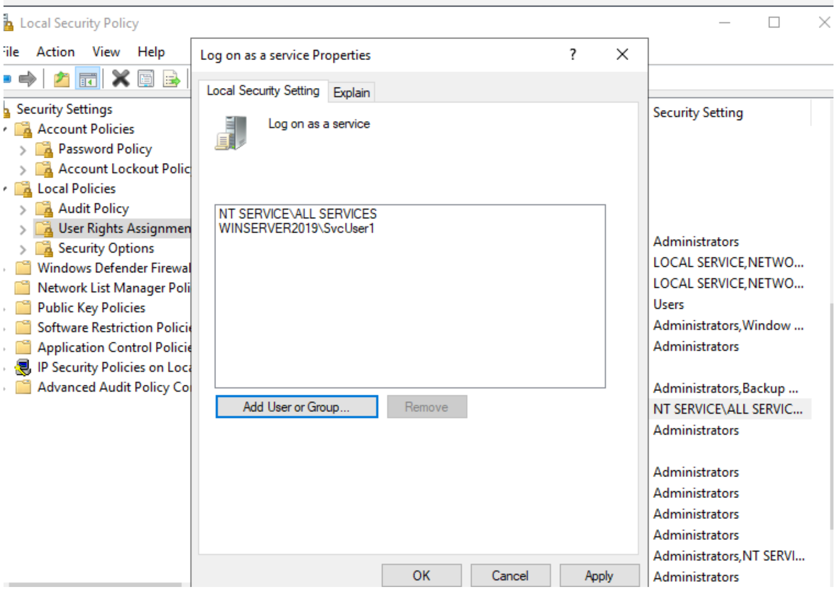
| Policy | Security Setting |
|---|---|
| Enforce password history | 5 passwords remembered |
| Maximum password age | 90 days |
| Minimum password age | 7 days |
| Minimum password length | 12 characters |
| Minimum password length audit | Not Defined |
| Password must meet complexity requirements | Enabled |
| Store passwords using reversible encryption | Disabled |

2.3 User Rights Assignment:

**ecpol.msc** ไปที่ **Local Policies > User Rights Assignment** เพื่อกำหนดสิทธิ์:

- **Log on as a service**: กำหนดให้เฉพาะบัญชีบริการ (เช่น SystemAdmin)
- **Log on locally**: กำหนดให้ DevUser1, TestUser1
- **Backup files and directories**: กำหนดให้กลุ่ม Backup Operators

ผลลัพธ์นี้จำกัดสิทธิ์การเข้าถึงตามบทบาทเพื่อลดความเสี่ยง

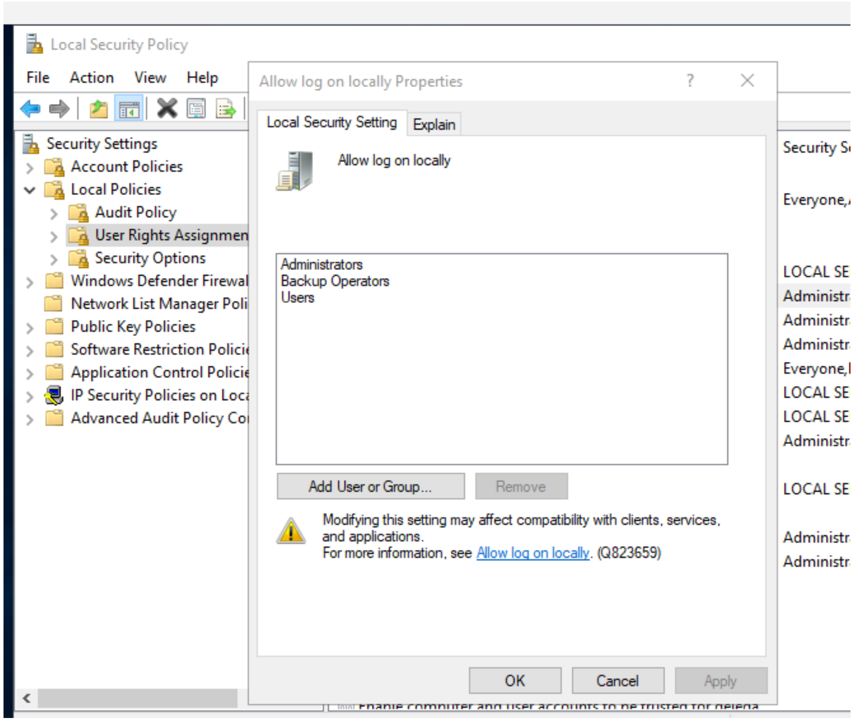


Log on as a service Properties

Log on as a service

NT SERVICE\ALL SERVICES
WINSERVER2019\SvcUser1

Administrators
LOCAL SERVICE,NETWO...
LOCAL SERVICE,NETWO...
Users
Administrators,Window ...
Administrators
Administrators,Backup ...
NT SERVICE\ALL SERVIC...
Administrators
Administrators
Administrators
Administrators
Administrators
Administrators,NT SERVI...
Administrators



Allow log on locally Properties

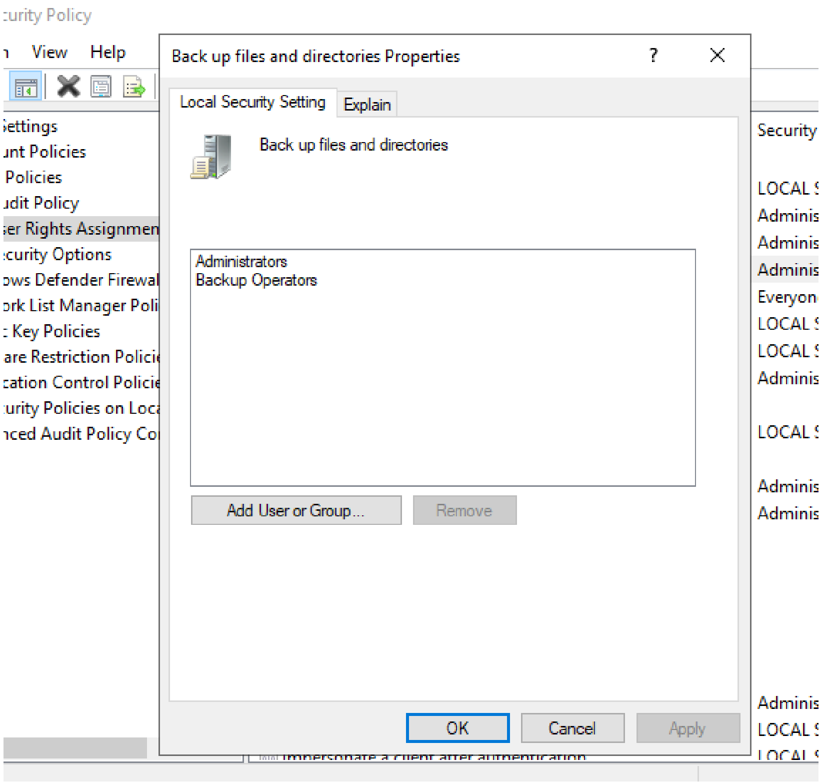
Allow log on locally

Administrators
Backup Operators
Users

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Allow log on locally. (Q823659)

Everyone,
LOCAL SE
Administr
Administr
Administr
Everyone,
LOCAL SE
LOCAL SE
Administr
LOCAL SE
Administr
Administr

Enable computer and user accounts to be trusted for delega



Back up files and directories Properties

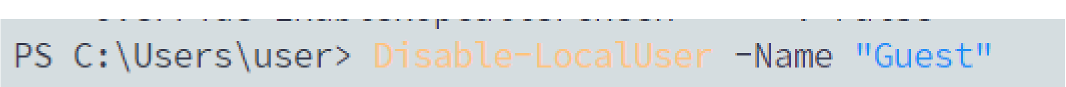
Local Security Setting | Explain

Back up files and directories

Administrators
Backup Operators

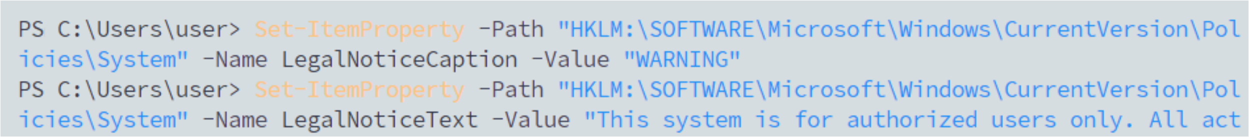
2.4 Security Options:

ปิดบัญชี Guest



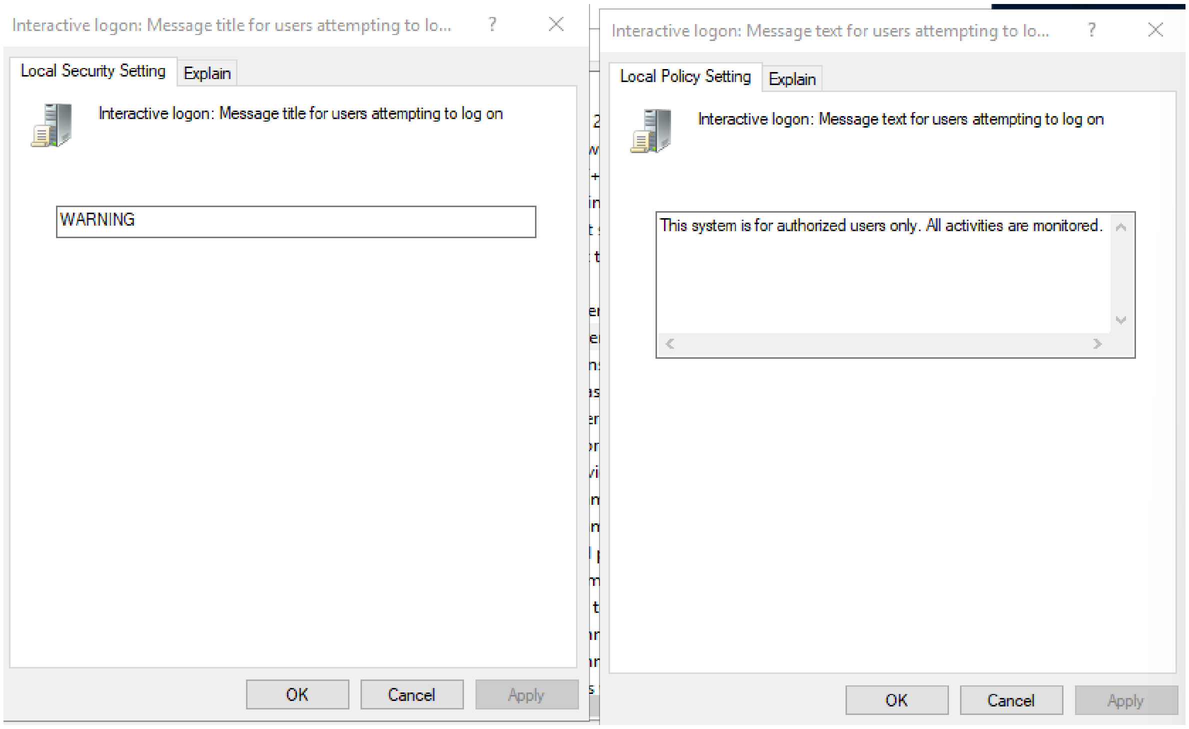
```
PS C:\Users\user> Disable-LocalUser -Name "Guest"
```

ตั้งข้อความ Logon:



```
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" -Name LegalNoticeCaption -Value "WARNING"
PS C:\Users\user> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol
icies\System" -Name LegalNoticeText -Value "This system is for authorized users only. All act
```

secpol.msc > Security Options แสดงการตั้งค่า Logon Message


Interactive logon: Message title for users attempting to lo...
?
Local Security Setting
Explain
OK
Cancel
Apply

Interactive logon: Message title for users attempting to log on

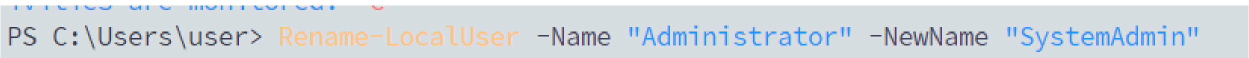
WARNING

Interactive logon: Message text for users attempting to lo...
?
Local Policy Setting
Explain
OK
Cancel
Apply

Interactive logon: Message text for users attempting to log on

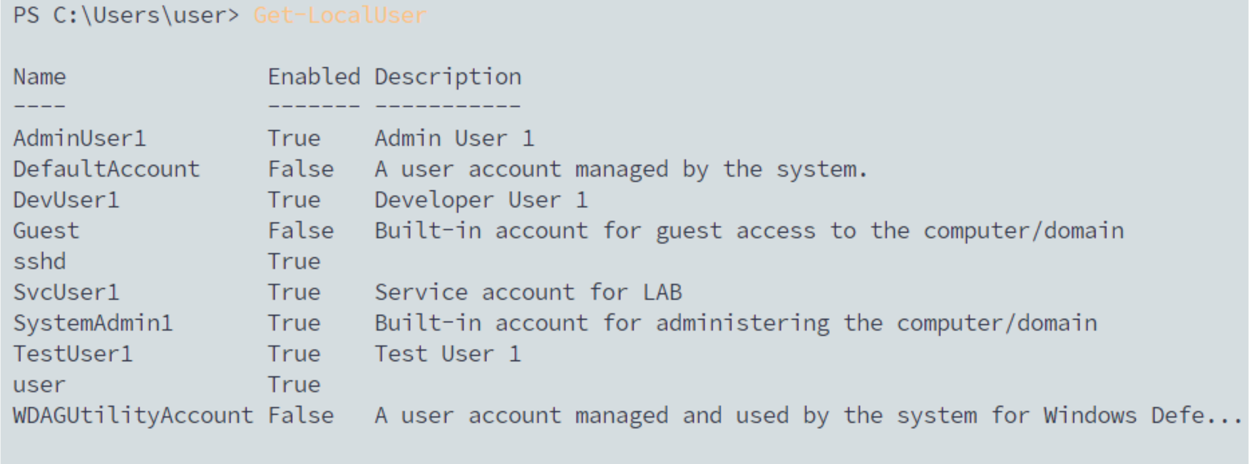
This system is for authorized users only. All activities are monitored.

เปลี่ยนชื่อ Administrator:



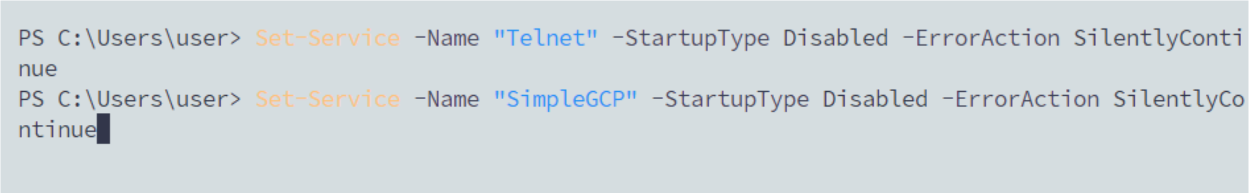
```
ivities are monitored.
PS C:\Users\user> Rename-LocalUser -Name "Administrator" -NewName "SystemAdmin"
```

ใช้ Get-LocalUser ผลลัพธ์การเปลี่ยนชื่อ Administrator เป็น SystemAdmin



```
PS C:\Users\user> Get-LocalUser

Name               Enabled Description
----               ------- -----------
AdminUser1         True    Admin User 1
DefaultAccount     False   A user account managed by the system.
DevUser1           True    Developer User 1
Guest              False   Built-in account for guest access to the computer/domain
sshd               True
SvcUser1           True    Service account for LAB
SystemAdmin1       True    Built-in account for administering the computer/domain
TestUser1          True    Test User 1
user               True
WDAGUtilityAccount False   A user account managed and used by the system for Windows Defe...
```

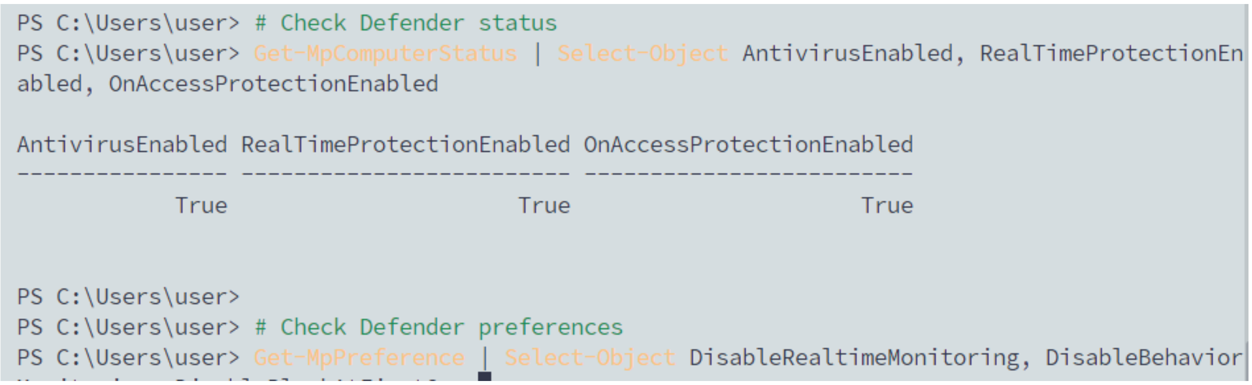
ปิดบริการที่ไม่จำเป็น



```
PS C:\Users\user> Set-Service -Name "Telnet" -StartupType Disabled -ErrorAction SilentlyConti
nue
PS C:\Users\user> Set-Service -Name "SimpleGCP" -StartupType Disabled -ErrorAction SilentlyCo
ntinue
```

## Task 3: Enable Windows Defender

### 3.1 Check Windows Defender Status:



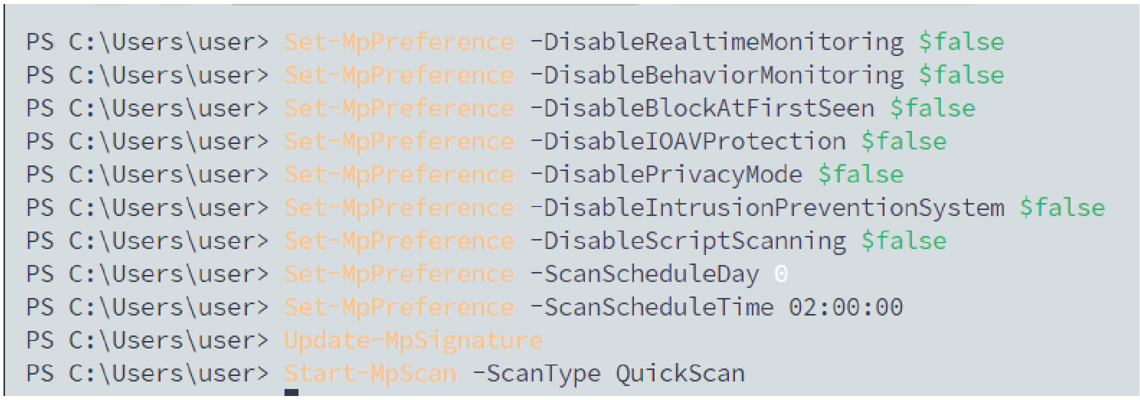
```
PS C:\Users\user> # Check Defender status
PS C:\Users\user> Get-MpComputerStatus | Select-Object AntivirusEnabled, RealTimeProtectionEn
abled, OnAccessProtectionEnabled

AntivirusEnabled RealTimeProtectionEnabled OnAccessProtectionEnabled
---------------- ------------------------- -------------------------
            True                      True                      True


PS C:\Users\user>
PS C:\Users\user> # Check Defender preferences
PS C:\Users\user> Get-MpPreference | Select-Object DisableRealtimeMonitoring, DisableBehavior
```

แสดงสถานะ:

- AntivirusEnabled: True (เปิดใช้งาน) หรือ False
- RealTimeProtectionEnabled: True (ป้องกันแบบเรียลไทม์) หรือ False
- OnAccessProtectionEnabled: True (ป้องกันเมื่อเข้าถึงไฟล์) หรือ False

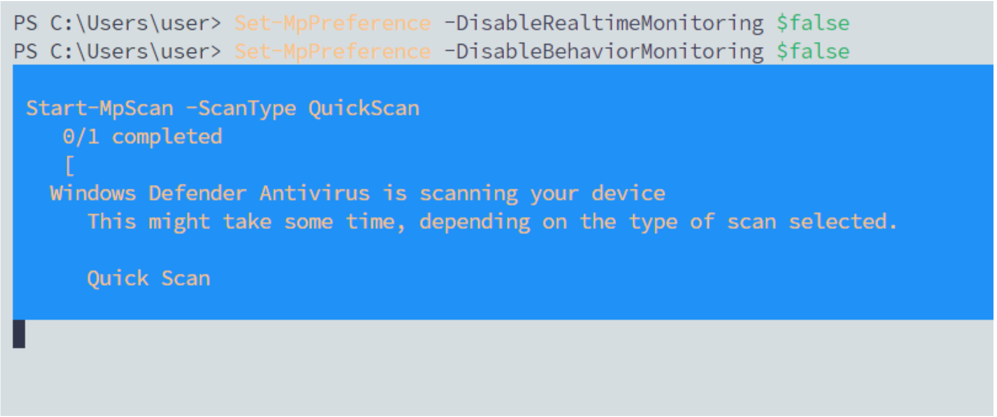
### 3.2 Configure Windows Defender:

**ค่าการตั้งค่า (ควรเป็น False = ไม่ได้ปิดฟีเจอร์)**

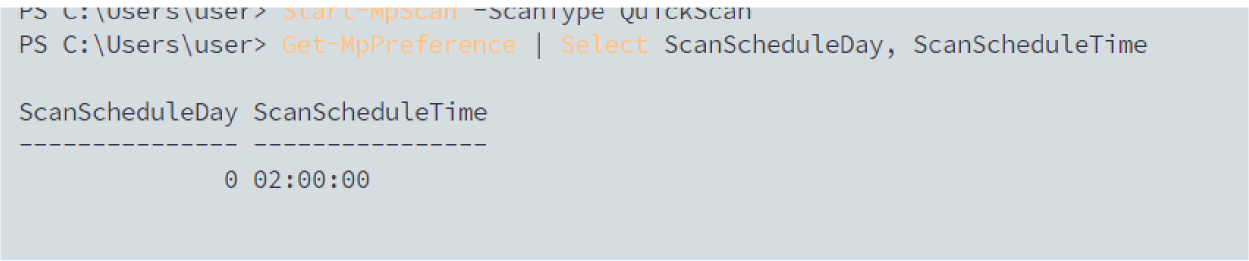


```
PS C:\Users\user> Set-MpPreference -DisableRealtimeMonitoring $false
PS C:\Users\user> Set-MpPreference -DisableBehaviorMonitoring $false
PS C:\Users\user> Set-MpPreference -DisableBlockAtFirstSeen $false
PS C:\Users\user> Set-MpPreference -DisableIOAVProtection $false
PS C:\Users\user> Set-MpPreference -DisablePrivacyMode $false
PS C:\Users\user> Set-MpPreference -DisableIntrusionPreventionSystem $false
PS C:\Users\user> Set-MpPreference -DisableScriptScanning $false
PS C:\Users\user> Set-MpPreference -ScanScheduleDay 0
PS C:\Users\user> Set-MpPreference -ScanScheduleTime 02:00:00
PS C:\Users\user> Update-MpSignature
PS C:\Users\user> Start-MpScan -ScanType QuickScan
```

- ทุกการตั้งค่า Disable* ถูกตั้งเป็น $false (เปิดใช้งาน)
- การสแกนตามกำหนดการถูกตั้งเป็นทุกวันเวลา 02:00 AM
- Update-MpSignature อัปเดตลายเซ็นต์ภัยคุกคาม (อาจใช้เวลาเล็กน้อย)
- Start-MpScan จะรัน Quick Scan และแสดงผลลัพธ์เมื่อเสร็จ

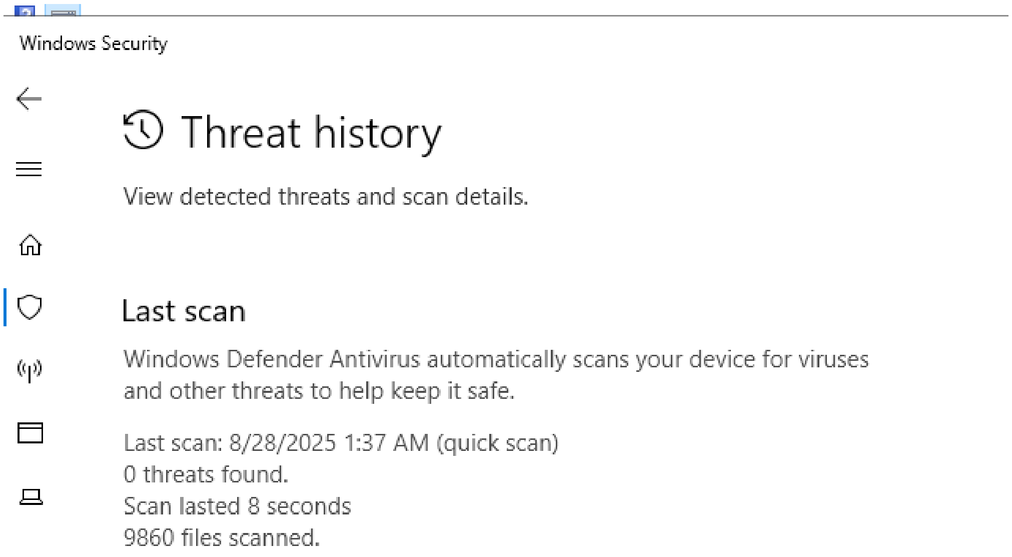


```
PS C:\Users\user> Set-MpPreference -DisableRealtimeMonitoring $false
PS C:\Users\user> Set-MpPreference -DisableBehaviorMonitoring $false

Start-MpScan -ScanType QuickScan
   0/1 completed
   [
  Windows Defender Antivirus is scanning your device
     This might take some time, depending on the type of scan selected.

     Quick Scan
```



```
PS C:\Users\user> Start-MpScan -ScanType QuickScan
PS C:\Users\user> Get-MpPreference | Select ScanScheduleDay, ScanScheduleTime

ScanScheduleDay ScanScheduleTime
--------------- ----------------
              0 02:00:00
```

การตั้งค่านี้เปิดใช้งานการป้องกันทั้งหมดและกำหนดการสแกนอัตโนมัติทุกวัน การอัปเดตลายเซ็นต์ช่วยให้ระบบตรวจจับภัยคุกคามล่าสุด



Windows Security

Threat history

View detected threats and scan details.

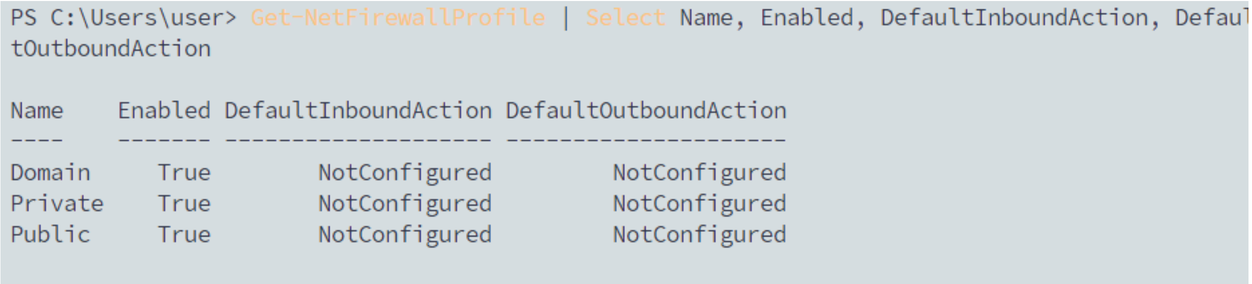
Last scan

Windows Defender Antivirus automatically scans your device for viruses and other threats to help keep it safe.

Last scan: 8/28/2025 1:37 AM (quick scan)
0 threats found.
Scan lasted 8 seconds
9860 files scanned.

### 3.3 Configure Windows Defender Firewall:

ดูสถานะโปรไฟล์ไฟร์วอลล์

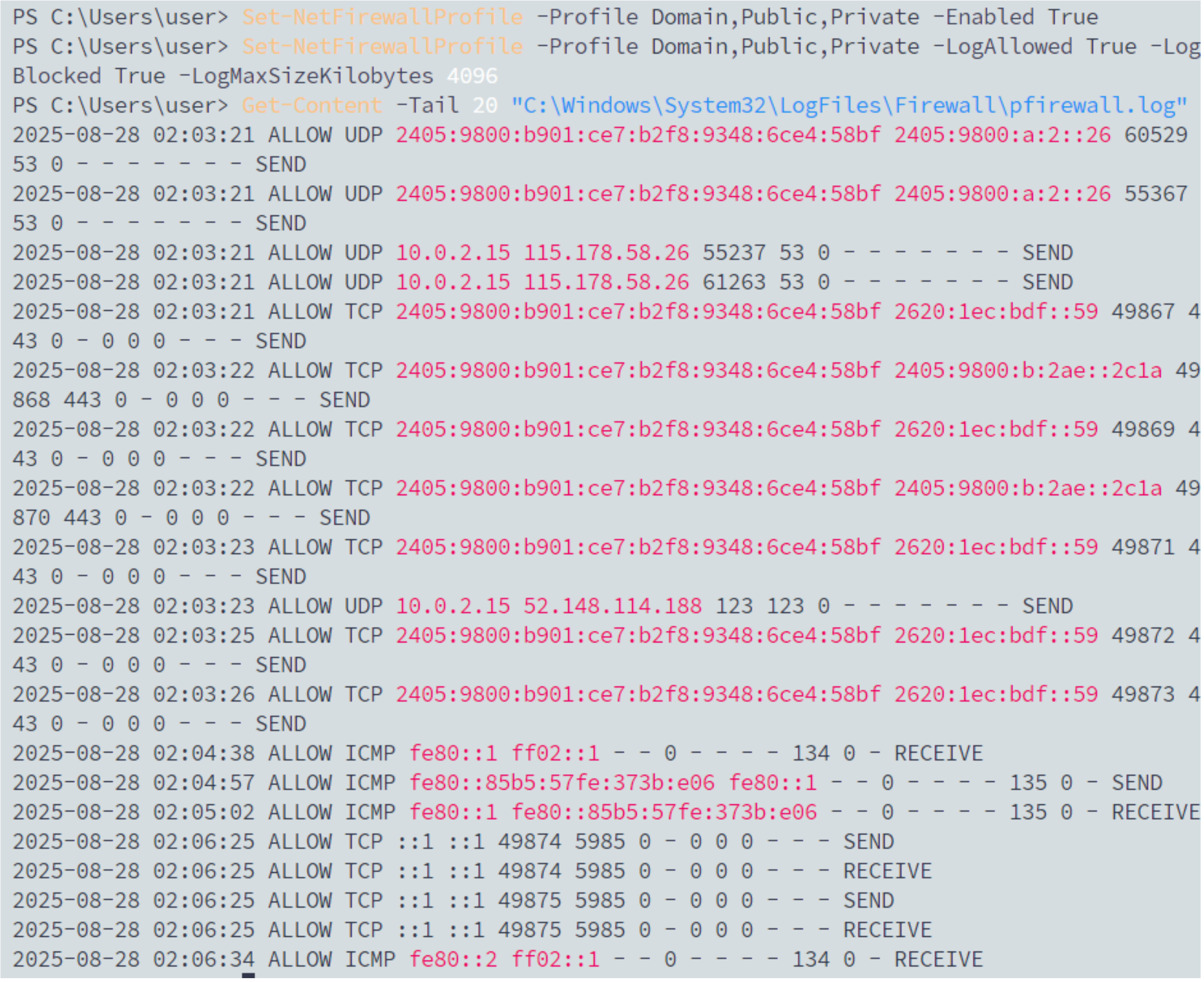


```
PS C:\Users\user> Get-NetFirewallProfile | Select Name, Enabled, DefaultInboundAction, Defaul
tOutboundAction

Name    Enabled DefaultInboundAction DefaultOutboundAction
----    ------- -------------------- ---------------------
Domain     True        NotConfigured         NotConfigured
Private    True        NotConfigured         NotConfigured
Public     True        NotConfigured         NotConfigured
```

- Get-NetFirewallProfile แสดงสถานะโปรไฟล์ (Domain, Private, Public) ก่อนตั้งค่า
- หลัง Set-NetFirewallProfile ทั้ง 3 โปรไฟล์จะเป็น Enabled: True

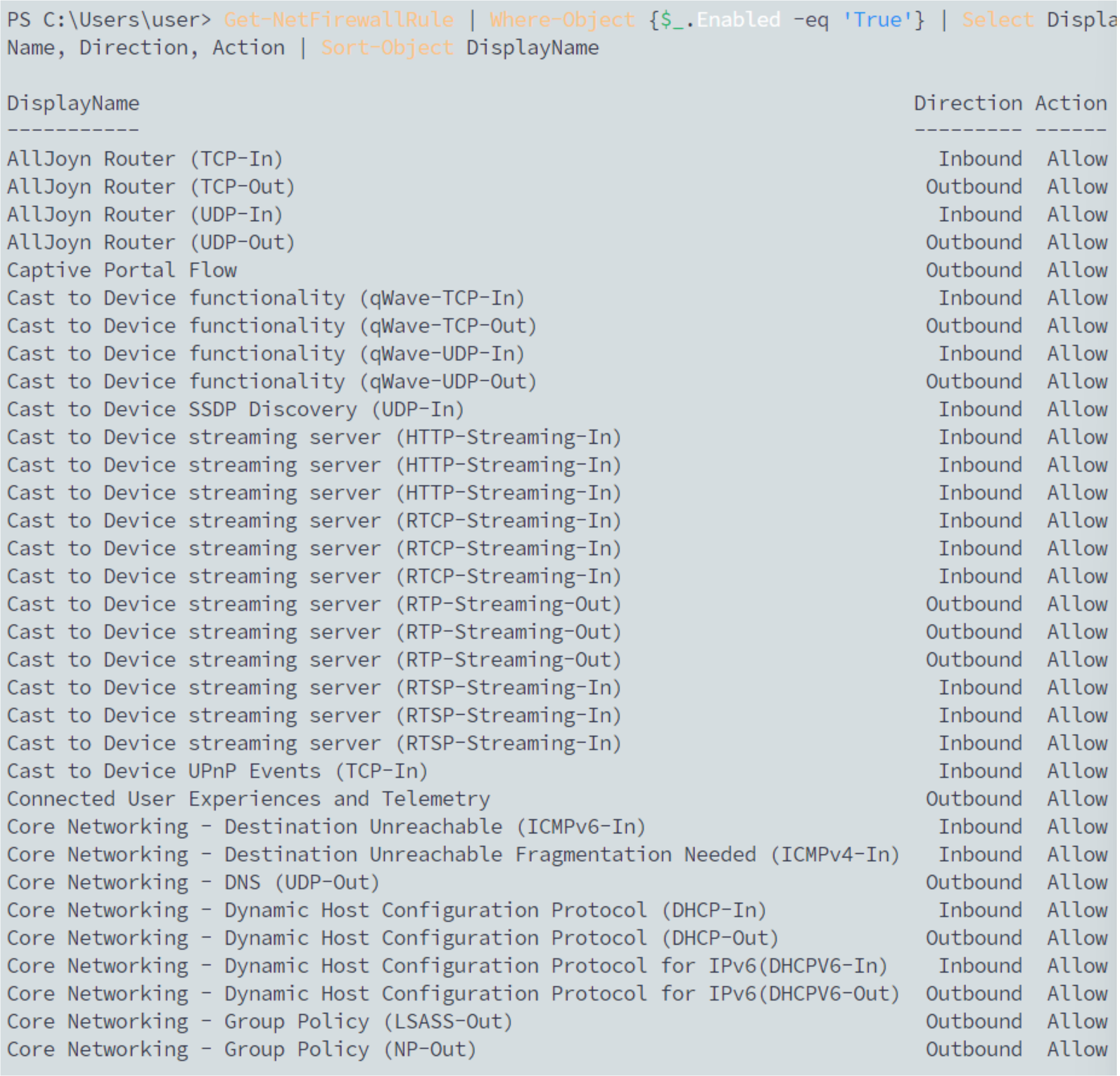
การเปิดใช้งาน Firewall ทั้ง 3 โปรไฟล์และการบันทึกเหตุการณ์ช่วยป้องกันการโจมตีจากเครือข่าย

เปิดทุกโปรไฟล์ // เปิดการ // Log ดูท้ายไฟล์ log



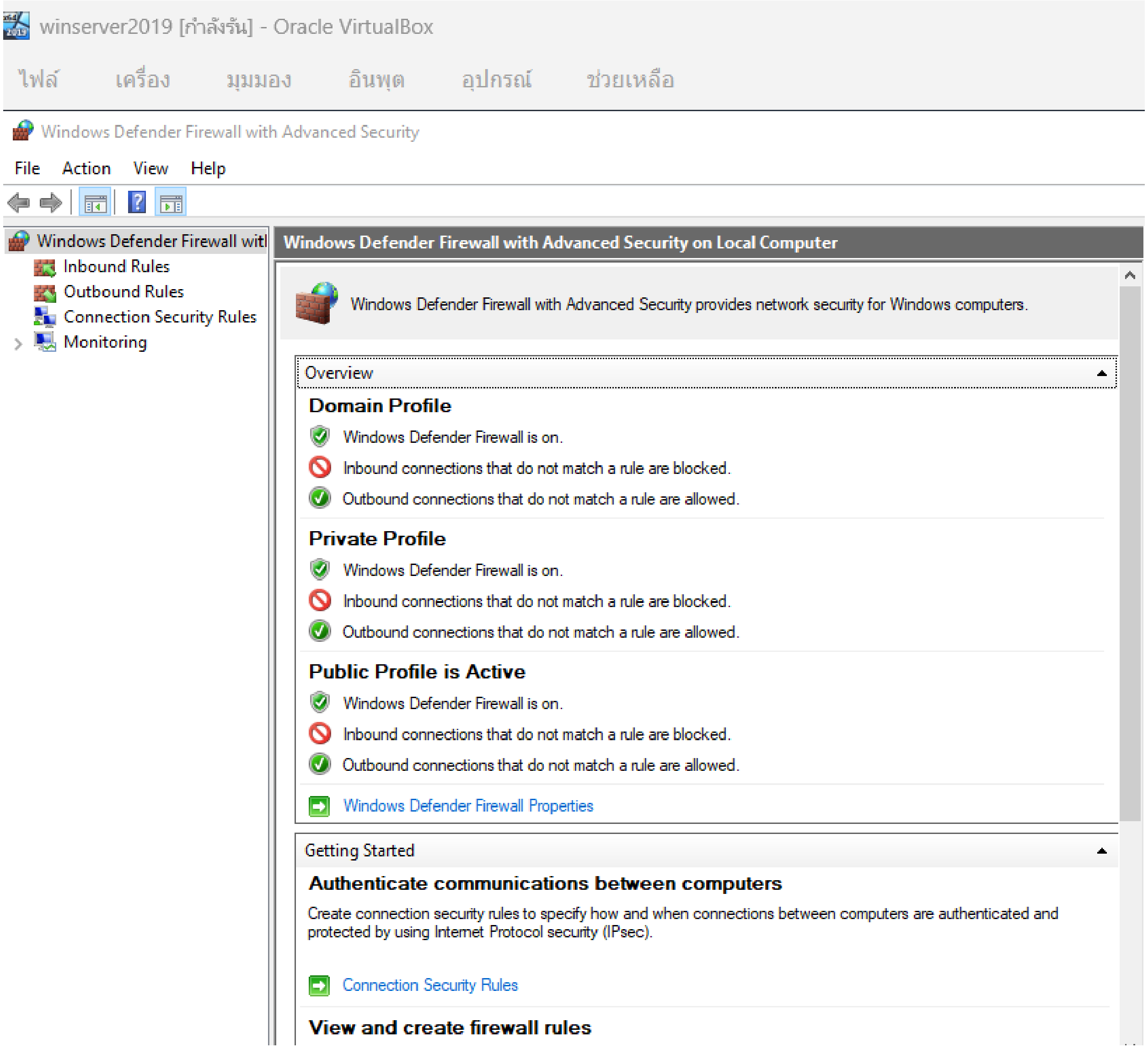
```
PS C:\Users\user> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
PS C:\Users\user> Set-NetFirewallProfile -Profile Domain,Public,Private -LogAllowed True -Log
Blocked True -LogMaxSizeKilobytes 4096
PS C:\Users\user> Get-Content -Tail 20 "C:\Windows\System32\LogFiles\Firewall\pfirewall.log"
2025-08-28 02:03:21 ALLOW UDP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2405:9800:a:2::26 60529
53 0 - - - - - - - SEND
2025-08-28 02:03:21 ALLOW UDP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2405:9800:a:2::26 55367
53 0 - - - - - - - SEND
2025-08-28 02:03:21 ALLOW UDP 10.0.2.15 115.178.58.26 55237 53 0 - - - - - - - SEND
2025-08-28 02:03:21 ALLOW UDP 10.0.2.15 115.178.58.26 61263 53 0 - - - - - - - SEND
2025-08-28 02:03:21 ALLOW TCP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2620:1ec:bdf::59 49867 4
43 0 - 0 0 0 - - - SEND
2025-08-28 02:03:22 ALLOW TCP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2405:9800:b:2ae::2c1a 49
868 443 0 - 0 0 0 - - - SEND
2025-08-28 02:03:22 ALLOW TCP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2620:1ec:bdf::59 49869 4
43 0 - 0 0 0 - - - SEND
2025-08-28 02:03:22 ALLOW TCP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2405:9800:b:2ae::2c1a 49
870 443 0 - 0 0 0 - - - SEND
2025-08-28 02:03:23 ALLOW TCP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2620:1ec:bdf::59 49871 4
43 0 - 0 0 0 - - - SEND
2025-08-28 02:03:23 ALLOW UDP 10.0.2.15 52.148.114.188 123 123 0 - - - - - - - SEND
2025-08-28 02:03:25 ALLOW TCP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2620:1ec:bdf::59 49872 4
43 0 - 0 0 0 - - - SEND
2025-08-28 02:03:26 ALLOW TCP 2405:9800:b901:ce7:b2f8:9348:6ce4:58bf 2620:1ec:bdf::59 49873 4
43 0 - 0 0 0 - - - SEND
2025-08-28 02:04:38 ALLOW ICMP fe80::1 ff02::1 - - 0 - - - - 134 0 - RECEIVE
2025-08-28 02:04:57 ALLOW ICMP fe80::85b5:57fe:373b:e06 fe80::1 - - 0 - - - - 135 0 - SEND
2025-08-28 02:05:02 ALLOW ICMP fe80::1 fe80::85b5:57fe:373b:e06 - - 0 - - - - 135 0 - RECEIVE
2025-08-28 02:06:25 ALLOW TCP ::1 ::1 49874 5985 0 - 0 0 0 - - - SEND
2025-08-28 02:06:25 ALLOW TCP ::1 ::1 49874 5985 0 - 0 0 0 - - - RECEIVE
2025-08-28 02:06:25 ALLOW TCP ::1 ::1 49875 5985 0 - 0 0 0 - - - SEND
2025-08-28 02:06:25 ALLOW TCP ::1 ::1 49875 5985 0 - 0 0 0 - - - RECEIVE
2025-08-28 02:06:34 ALLOW ICMP fe80::2 ff02::1 - - 0 - - - - 134 0 - RECEIVE
```

(ตัวเลือก) รายการกฎที่เปิดใช้งาน



```
PS C:\Users\user> Get-NetFirewallRule | Where-Object {$_.Enabled -eq 'True'} | Select Displa
Name, Direction, Action | Sort-Object DisplayName

DisplayName                                                                  Direction Action
-----------                                                                  --------- ------
AllJoyn Router (TCP-In)                                                        Inbound  Allow
AllJoyn Router (TCP-Out)                                                      Outbound  Allow
AllJoyn Router (UDP-In)                                                        Inbound  Allow
AllJoyn Router (UDP-Out)                                                      Outbound  Allow
Captive Portal Flow                                                           Outbound  Allow
Cast to Device functionality (qWave-TCP-In)                                    Inbound  Allow
Cast to Device functionality (qWave-TCP-Out)                                  Outbound  Allow
Cast to Device functionality (qWave-UDP-In)                                    Inbound  Allow
Cast to Device functionality (qWave-UDP-Out)                                  Outbound  Allow
Cast to Device SSDP Discovery (UDP-In)                                         Inbound  Allow
Cast to Device streaming server (HTTP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (HTTP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (HTTP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (RTCP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (RTCP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (RTCP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (RTP-Streaming-Out)                           Outbound  Allow
Cast to Device streaming server (RTP-Streaming-Out)                           Outbound  Allow
Cast to Device streaming server (RTP-Streaming-Out)                           Outbound  Allow
Cast to Device streaming server (RTSP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (RTSP-Streaming-In)                            Inbound  Allow
Cast to Device streaming server (RTSP-Streaming-In)                            Inbound  Allow
Cast to Device UPnP Events (TCP-In)                                            Inbound  Allow
Connected User Experiences and Telemetry                                      Outbound  Allow
Core Networking - Destination Unreachable (ICMPv6-In)                          Inbound  Allow
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)     Inbound  Allow
Core Networking - DNS (UDP-Out)                                               Outbound  Allow
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)                Inbound  Allow
Core Networking - Dynamic Host Configuration Protocol (DHCP-Out)              Outbound  Allow
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)      Inbound  Allow
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)    Outbound  Allow
Core Networking - Group Policy (LSASS-Out)                                    Outbound  Allow
Core Networking - Group Policy (NP-Out)                                       Outbound  Allow
```

**Windows Defender Firewall with Advanced Security → Overview** (ทั้ง 3 โปรไฟล์เป็น **On**


winserver2019 [กำลังรัน] - Oracle VirtualBox
ไฟล์
เครื่อง
มุมมอง
อินพุต
อุปกรณ์
ช่วยเหลือ
Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows Defender Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Defender Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

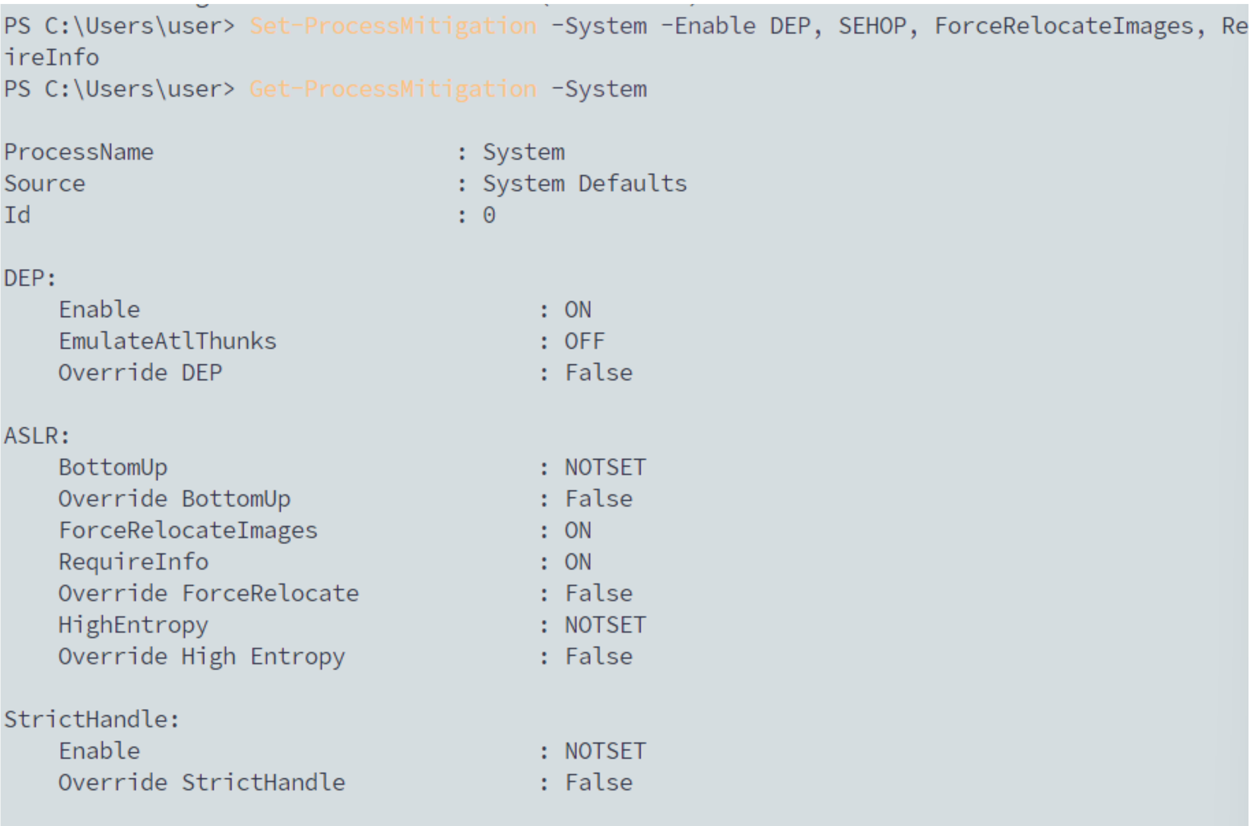
View and create firewall rules

## 3.4 Advanced Threat Protection

**Set-ProcessMitigation เปิดใช้งาน DEP, SEHOP, ForceRelocateImages, RequireInfo เพื่อป้องกันการโจมตีแบบ Exploi**

**Get-ProcessMitigation -System แสดงสถานะการตั้งค่า Exploit Protection**

การป้องกันขั้นสูงนี้ช่วยลดความเสี่ยงจากมัลแวร์ที่ใช้ช่องโหว่ซอฟต์แวร์

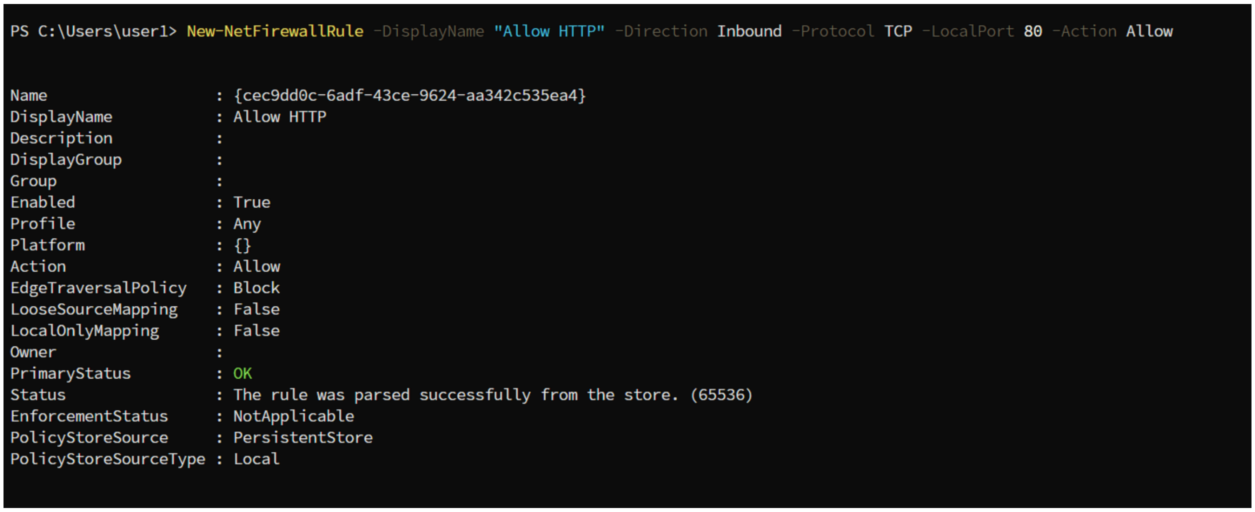


```
PS C:\Users\user> Set-ProcessMitigation -System -Enable DEP, SEHOP, ForceRelocateImages, Re
ireInfo
PS C:\Users\user> Get-ProcessMitigation -System

ProcessName                       : System
Source                            : System Defaults
Id                                : 0

DEP:
    Enable                              : ON
    EmulateAtlThunks                    : OFF
    Override DEP                        : False

ASLR:
    BottomUp                            : NOTSET
    Override BottomUp                   : False
    ForceRelocateImages                 : ON
    RequireInfo                         : ON
    Override ForceRelocate              : False
    HighEntropy                         : NOTSET
    Override High Entropy               : False

StrictHandle:
    Enable                              : NOTSET
    Override StrictHandle               : False
```

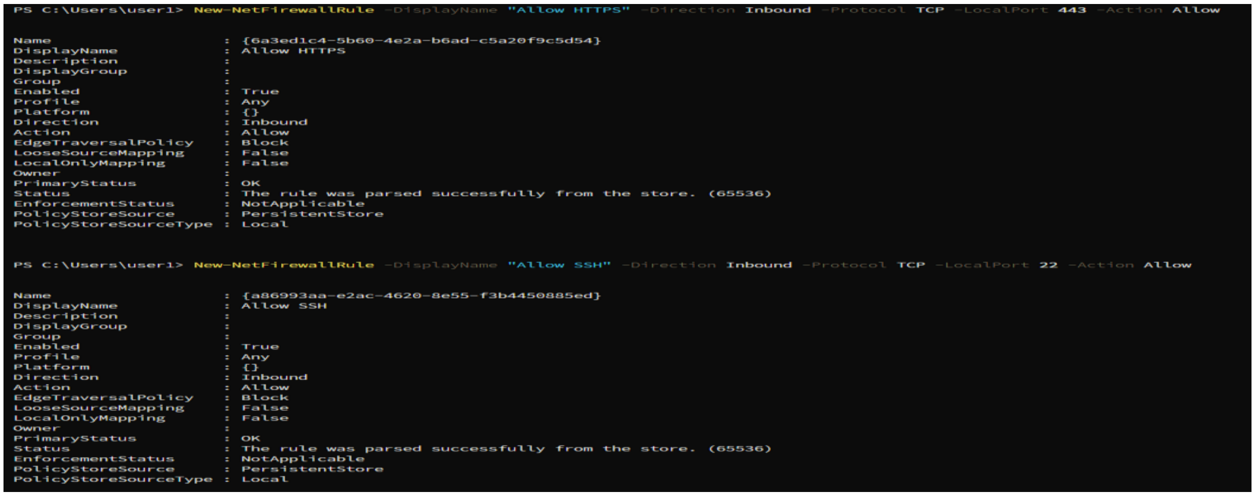
## Task 4: Configure Firewall Rules

### 4.1 Basic Firewall Configuration

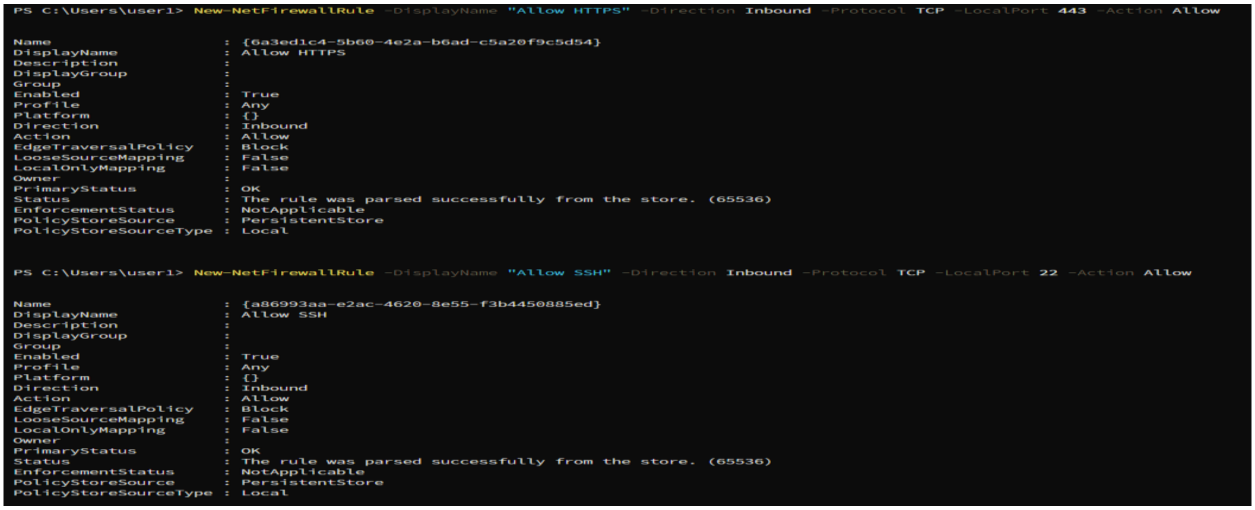
สร้าง Inbound Rules



```
PS C:\Users\user1> New-NetFirewallRule -DisplayName "Allow HTTP" -Direction Inbound -Protocol TCP -LocalPort 80 -Action Allow


Name                  : {cec9dd0c-6adf-43ce-9624-aa342c535ea4}
DisplayName           : Allow HTTP
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

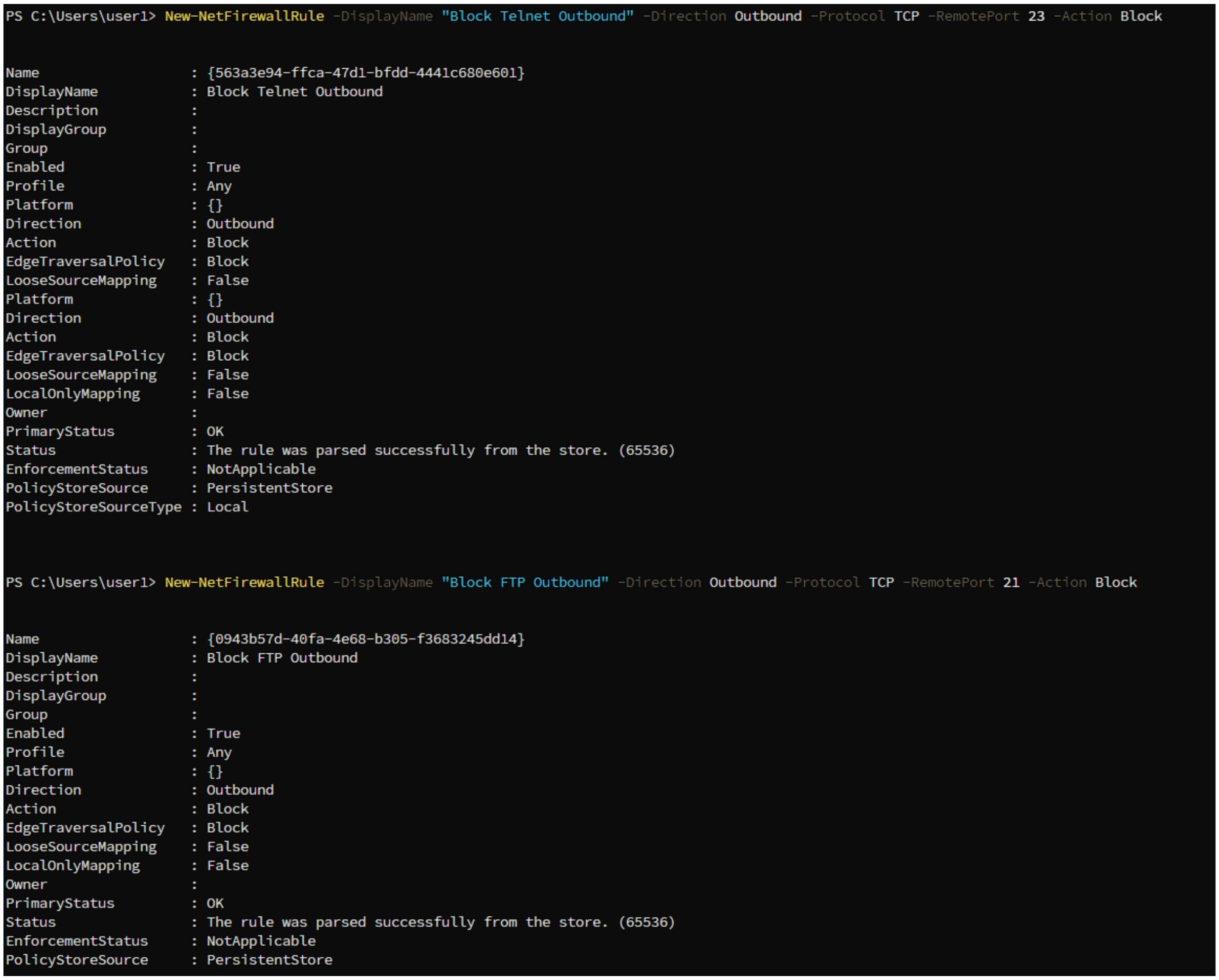


```
PS C:\Users\user1> New-NetFirewallRule -DisplayName "Allow HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow


Name                  : {6a3ed1c4-5b60-4e2a-b6ad-c5a20f9c5d54}
DisplayName           : Allow HTTPS
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local


PS C:\Users\user1> New-NetFirewallRule -DisplayName "Allow SSH" -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow


Name                  : {a86993aa-e2ac-4620-8e55-f3b4450885ed}
DisplayName           : Allow SSH
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```



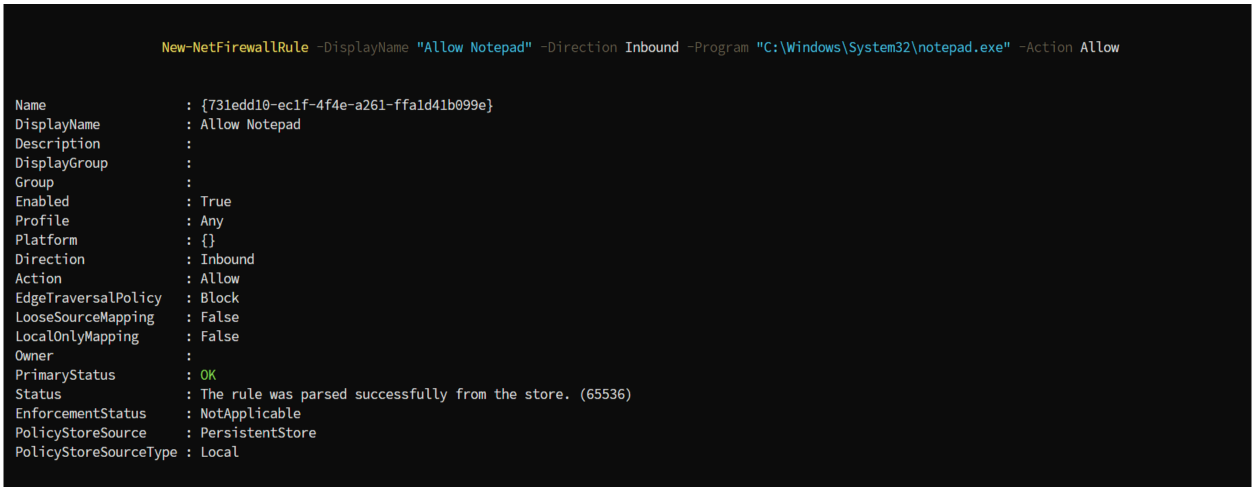
```
PS C:\Users\user1> New-NetFirewallRule -DisplayName "Allow HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow

Name                  : {6a3ed1c4-5b60-4e2a-b6ad-c5a20f9c5d54}
DisplayName           : Allow HTTPS
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local


PS C:\Users\user1> New-NetFirewallRule -DisplayName "Allow SSH" -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow

Name                  : {a86993aa-e2ac-4620-8e55-f3b4450885ed}
DisplayName           : Allow SSH
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

สร้าง Outbound Rules



```
PS C:\Users\user1> New-NetFirewallRule -DisplayName "Block Telnet Outbound" -Direction Outbound -Protocol TCP -RemotePort 23 -Action Block


Name                  : {563a3e94-ffca-47d1-bfdd-4441c680e601}
DisplayName           : Block Telnet Outbound
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Outbound
Action                : Block
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
Platform              : {}
Direction             : Outbound
Action                : Block
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local



PS C:\Users\user1> New-NetFirewallRule -DisplayName "Block FTP Outbound" -Direction Outbound -Protocol TCP -RemotePort 21 -Action Block


Name                  : {0943b57d-40fa-4e68-b305-f3683245dd14}
DisplayName           : Block FTP Outbound
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Outbound
Action                : Block
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
```

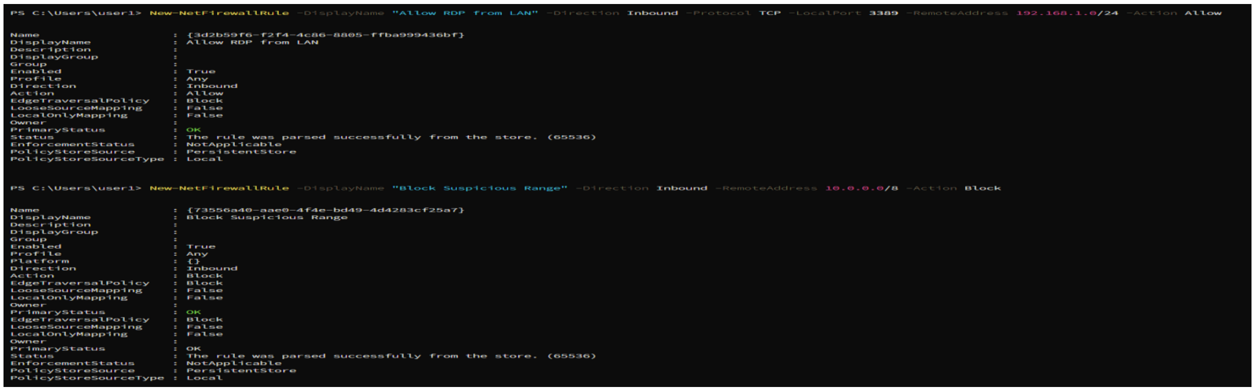
### Allow specific applications



```
              New-NetFirewallRule -DisplayName "Allow Notepad" -Direction Inbound -Program "C:\Windows\System32\notepad.exe" -Action Allow


Name                  : {731edd10-ec1f-4f4e-a261-ffa1d41b099e}
DisplayName           : Allow Notepad
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

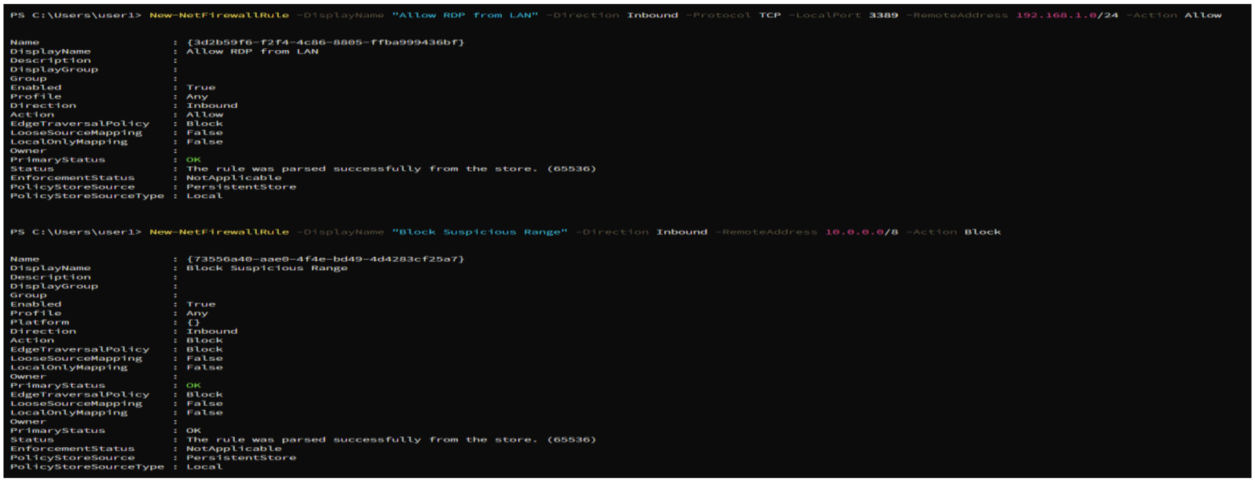
## 4.2 Advanced Firewall Rules:

### จำกัด Source IP (Allow RDP เฉพาะ LAN)



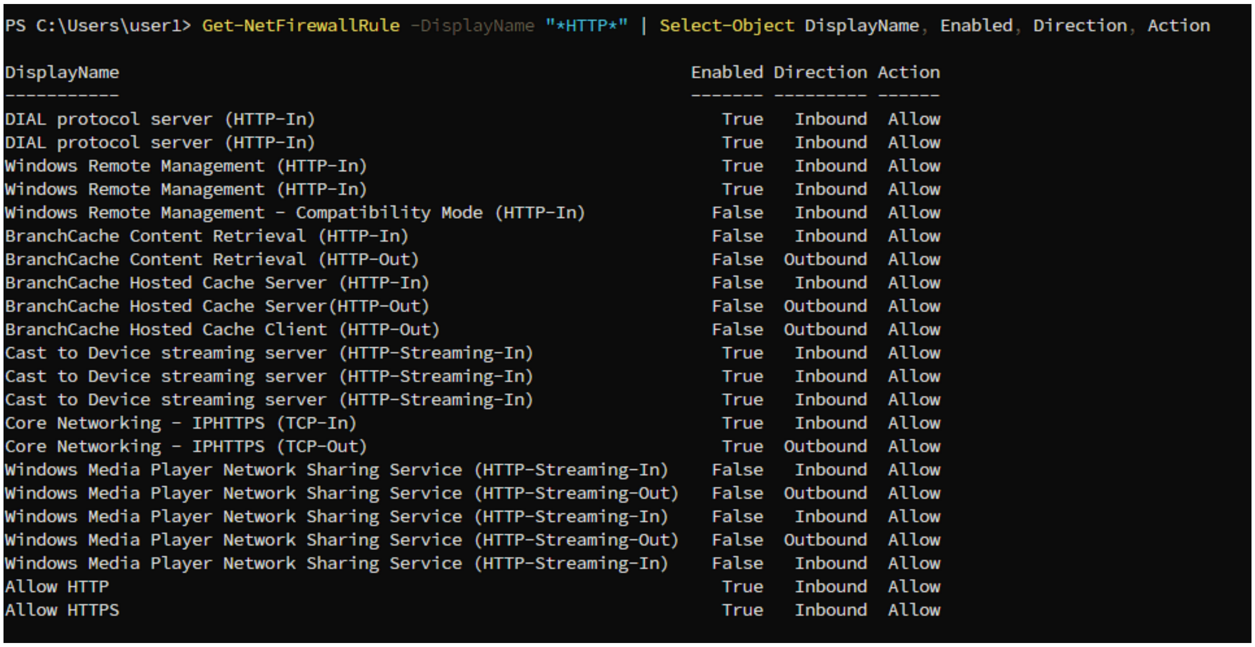
```
PS C:\Users\user1> New-NetFirewallRule -DisplayName "Allow RDP from LAN" -Direction Inbound -Protocol TCP -LocalPort 3389 -RemoteAddress 192.168.1.0/24 -Action Allow

Name                  : {3d2b59f6-f2f4-4c86-8805-ffba999436bf}
DisplayName           : Allow RDP from LAN
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local


PS C:\Users\user1> New-NetFirewallRule -DisplayName "Block Suspicious Range" -Direction Inbound -RemoteAddress 10.0.0.0/8 -Action Block

Name                  : {73556a40-aae0-4f4e-bd49-4d4283cf25a7}
DisplayName           : Block Suspicious Range
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Block
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

### Block IP Range



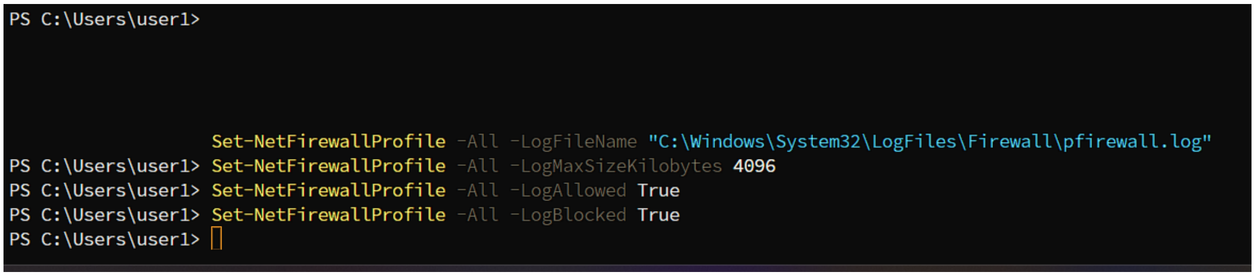
```
PS C:\Users\user1> New-NetFirewallRule -DisplayName "Allow RDP from LAN" -Direction Inbound -Protocol TCP -LocalPort 3389 -RemoteAddress 192.168.1.0/24 -Action Allow

Name                  : {3d2b59f6-f2f4-4c86-8805-ffba999436bf}
DisplayName           : Allow RDP from LAN
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local


PS C:\Users\user1> New-NetFirewallRule -DisplayName "Block Suspicious Range" -Direction Inbound -RemoteAddress 10.0.0.0/8 -Action Block

Name                  : {73556a40-aae0-4f4e-bd49-4d4283cf25a7}
DisplayName           : Block Suspicious Range
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Block
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

ตรวจสอบ Rule ที่สร้าง



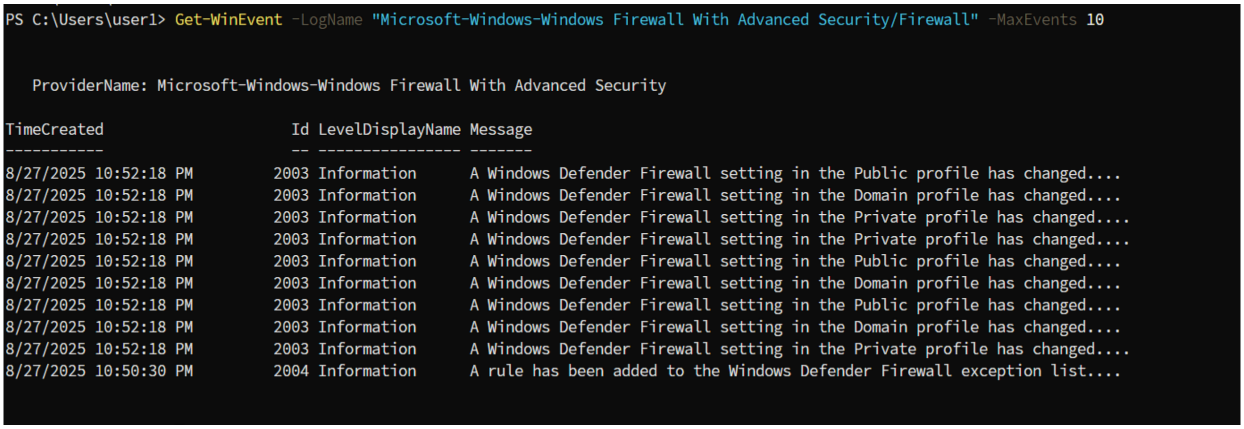
```
PS C:\Users\user1> Get-NetFirewallRule -DisplayName "*HTTP*" | Select-Object DisplayName, Enabled, Direction, Action

DisplayName                                                     Enabled Direction Action
-----------                                                     ------- --------- ------
DIAL protocol server (HTTP-In)                                     True   Inbound  Allow
DIAL protocol server (HTTP-In)                                     True   Inbound  Allow
Windows Remote Management (HTTP-In)                                True   Inbound  Allow
Windows Remote Management (HTTP-In)                                True   Inbound  Allow
Windows Remote Management - Compatibility Mode (HTTP-In)          False   Inbound  Allow
BranchCache Content Retrieval (HTTP-In)                           False   Inbound  Allow
BranchCache Content Retrieval (HTTP-Out)                          False  Outbound  Allow
BranchCache Hosted Cache Server (HTTP-In)                         False   Inbound  Allow
BranchCache Hosted Cache Server(HTTP-Out)                         False  Outbound  Allow
BranchCache Hosted Cache Client (HTTP-Out)                        False  Outbound  Allow
Cast to Device streaming server (HTTP-Streaming-In)                True   Inbound  Allow
Cast to Device streaming server (HTTP-Streaming-In)                True   Inbound  Allow
Cast to Device streaming server (HTTP-Streaming-In)                True   Inbound  Allow
Core Networking - IPHTTPS (TCP-In)                                 True   Inbound  Allow
Core Networking - IPHTTPS (TCP-Out)                                True  Outbound  Allow
Windows Media Player Network Sharing Service (HTTP-Streaming-In)  False   Inbound  Allow
Windows Media Player Network Sharing Service (HTTP-Streaming-Out) False  Outbound  Allow
Windows Media Player Network Sharing Service (HTTP-Streaming-In)  False   Inbound  Allow
Windows Media Player Network Sharing Service (HTTP-Streaming-Out) False  Outbound  Allow
Windows Media Player Network Sharing Service (HTTP-Streaming-In)  False   Inbound  Allow
Allow HTTP                                                         True   Inbound  Allow
Allow HTTPS                                                        True   Inbound  Allow
```

เปิด Firewall Logging



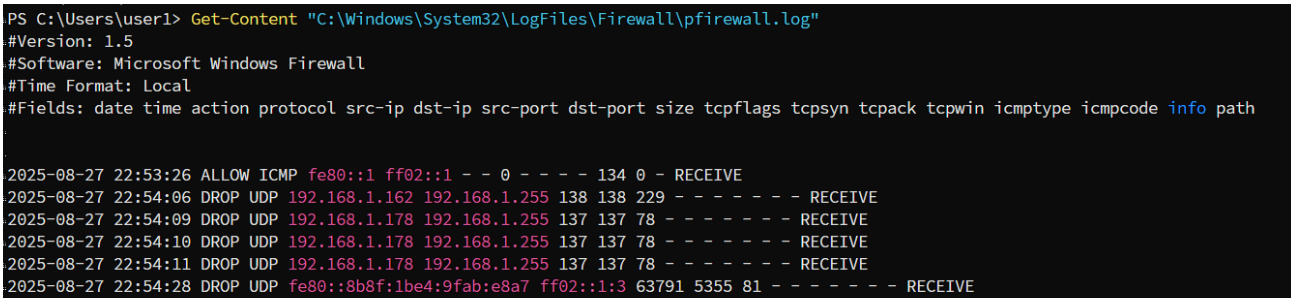
```
PS C:\Users\user1>



                    Set-NetFirewallProfile -All -LogFileName "C:\Windows\System32\LogFiles\Firewall\pfirewall.log"
PS C:\Users\user1> Set-NetFirewallProfile -All -LogMaxSizeKilobytes 4096
PS C:\Users\user1> Set-NetFirewallProfile -All -LogAllowed True
PS C:\Users\user1> Set-NetFirewallProfile -All -LogBlocked True
PS C:\Users\user1>
```

ดู Log ล่าสุด



```
PS C:\Users\user1> Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 10


   ProviderName: Microsoft-Windows-Windows Firewall With Advanced Security

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Public profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Domain profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Private profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Private profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Public profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Domain profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Public profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Domain profile has changed....
8/27/2025 10:52:18 PM         2003 Information      A Windows Defender Firewall setting in the Private profile has changed....
8/27/2025 10:50:30 PM         2004 Information      A rule has been added to the Windows Defender Firewall exception list....
```

เปิดไฟล์ pfirewall.log ใน PowerShell

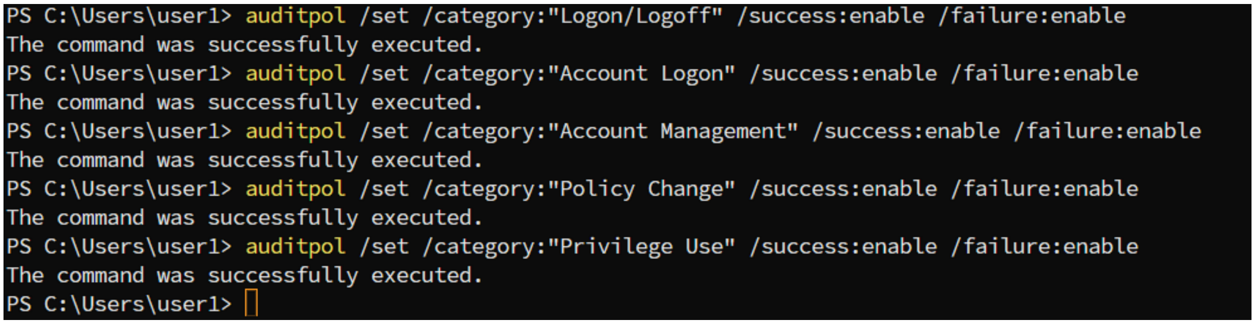


```
PS C:\Users\user1> Get-Content "C:\Windows\System32\LogFiles\Firewall\pfirewall.log"
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path


2025-08-27 22:53:26 ALLOW ICMP fe80::1 ff02::1 - - 0 - - - - 134 0 - RECEIVE
2025-08-27 22:54:06 DROP UDP 192.168.1.162 192.168.1.255 138 138 229 - - - - - - - RECEIVE
2025-08-27 22:54:09 DROP UDP 192.168.1.178 192.168.1.255 137 137 78 - - - - - - - RECEIVE
2025-08-27 22:54:10 DROP UDP 192.168.1.178 192.168.1.255 137 137 78 - - - - - - - RECEIVE
2025-08-27 22:54:11 DROP UDP 192.168.1.178 192.168.1.255 137 137 78 - - - - - - - RECEIVE
2025-08-27 22:54:28 DROP UDP fe80::8b8f:1be4:9fab:e8a7 ff02::1:3 63791 5355 81 - - - - - - - RECEIVE
```

## Task 5: Set up Event Monitoring

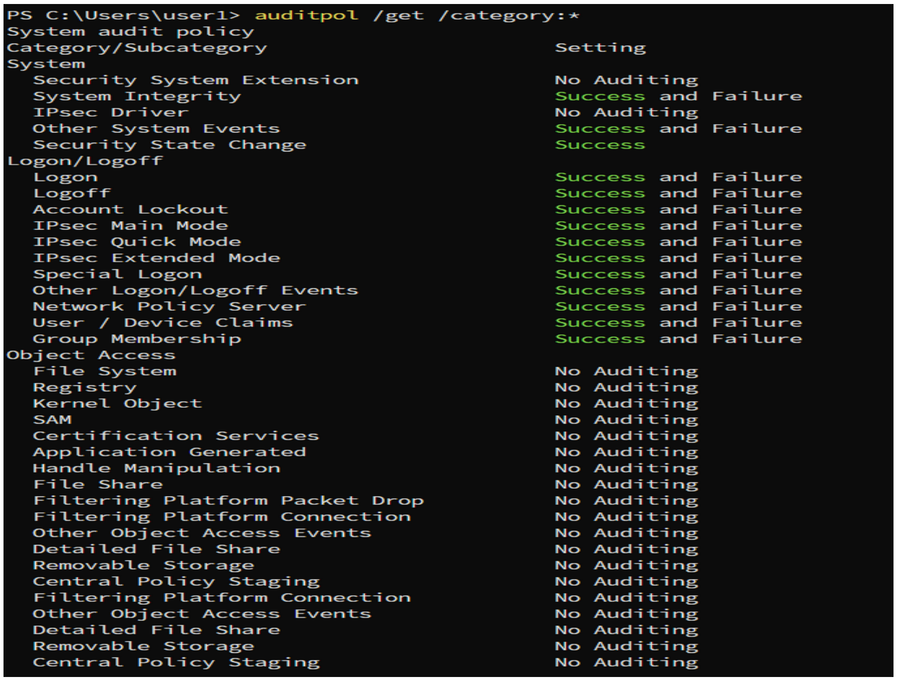
Configure Event Logging

เปิด PowerShell (Admin) แล้วรัน



```
PS C:\Users\user1> auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
The command was successfully executed.
PS C:\Users\user1> auditpol /set /category:"Account Logon" /success:enable /failure:enable
The command was successfully executed.
PS C:\Users\user1> auditpol /set /category:"Account Management" /success:enable /failure:enable
The command was successfully executed.
PS C:\Users\user1> auditpol /set /category:"Policy Change" /success:enable /failure:enable
The command was successfully executed.
PS C:\Users\user1> auditpol /set /category:"Privilege Use" /success:enable /failure:enable
The command was successfully executed.
PS C:\Users\user1> 
```

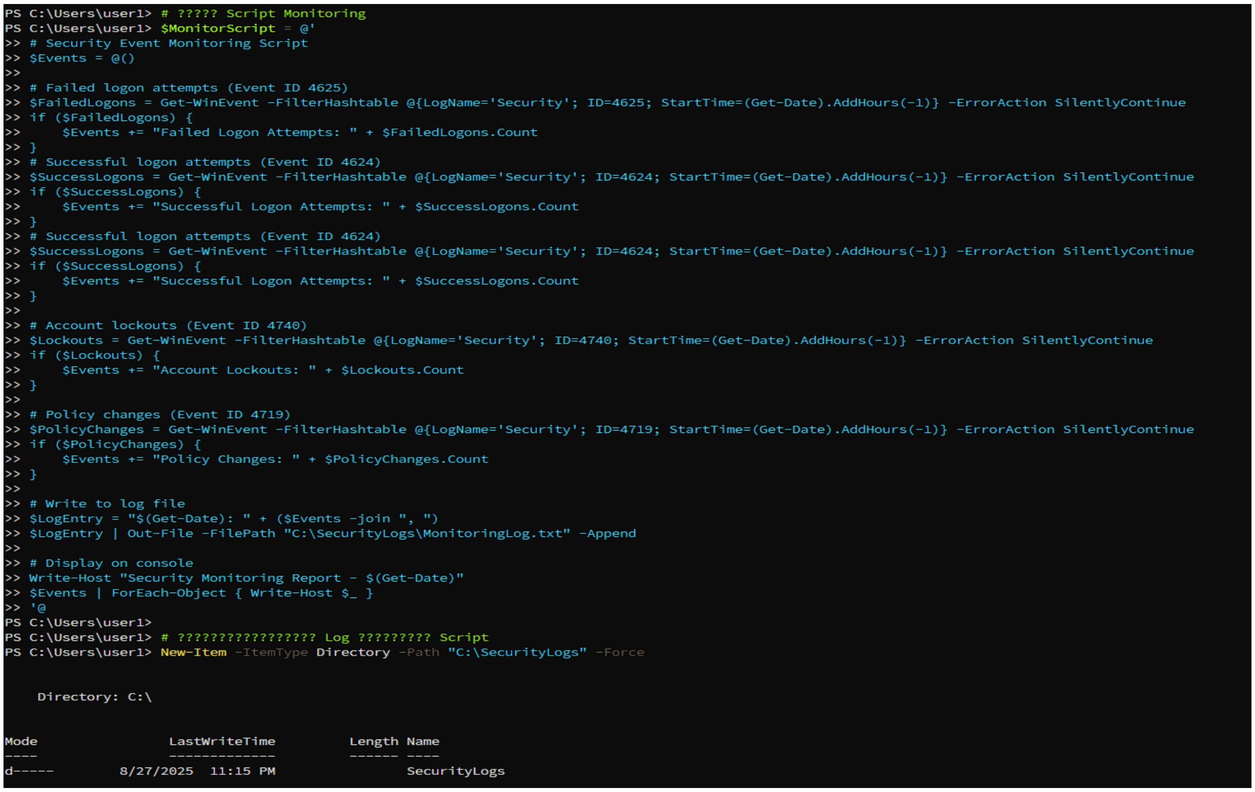
ตรวจสอบว่าตั้งค่านโยบาย Audit แล้วหรือยัง



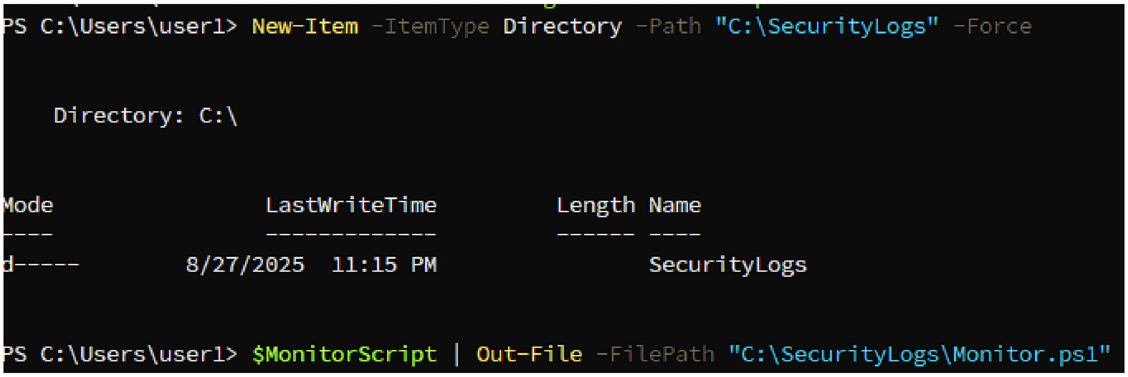
```
PS C:\Users\user1> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
  Group Membership                        Success and Failure
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
```

## Monitor Security Events

สร้างสคริปต์ตรวจจับ Event Security

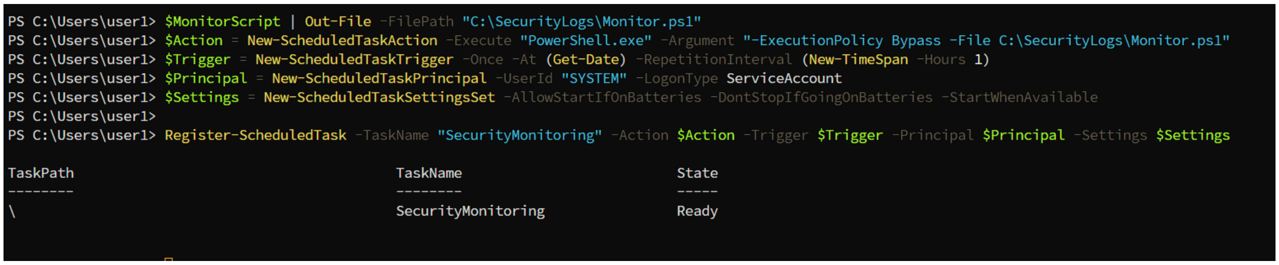


```
PS C:\Users\user1> # ????? Script Monitoring
PS C:\Users\user1> $MonitorScript = @'
>> # Security Event Monitoring Script
>> $Events = @()
>>
>> # Failed logon attempts (Event ID 4625)
>> $FailedLogons = Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625; StartTime=(Get-Date).AddHours(-1)} -ErrorAction SilentlyContinue
>> if ($FailedLogons) {
>>     $Events += "Failed Logon Attempts: " + $FailedLogons.Count
>> }
>> # Successful logon attempts (Event ID 4624)
>> $SuccessLogons = Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4624; StartTime=(Get-Date).AddHours(-1)} -ErrorAction SilentlyContinue
>> if ($SuccessLogons) {
>>     $Events += "Successful Logon Attempts: " + $SuccessLogons.Count
>> }
>> # Successful logon attempts (Event ID 4624)
>> $SuccessLogons = Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4624; StartTime=(Get-Date).AddHours(-1)} -ErrorAction SilentlyContinue
>> if ($SuccessLogons) {
>>     $Events += "Successful Logon Attempts: " + $SuccessLogons.Count
>> }
>>
>> # Account lockouts (Event ID 4740)
>> $Lockouts = Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4740; StartTime=(Get-Date).AddHours(-1)} -ErrorAction SilentlyContinue
>> if ($Lockouts) {
>>     $Events += "Account Lockouts: " + $Lockouts.Count
>> }
>>
>> # Policy changes (Event ID 4719)
>> $PolicyChanges = Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4719; StartTime=(Get-Date).AddHours(-1)} -ErrorAction SilentlyContinue
>> if ($PolicyChanges) {
>>     $Events += "Policy Changes: " + $PolicyChanges.Count
>> }
>>
>> # Write to log file
>> $LogEntry = "$(Get-Date): " + ($Events -join ", ")
>> $LogEntry | Out-File -FilePath "C:\SecurityLogs\MonitoringLog.txt" -Append
>>
>> # Display on console
>> Write-Host "Security Monitoring Report - $(Get-Date)"
>> $Events | ForEach-Object { Write-Host $_ }
>> '@
PS C:\Users\user1>
PS C:\Users\user1> # ????????????????? Log ????????? Script
PS C:\Users\user1> New-Item -ItemType Directory -Path "C:\SecurityLogs" -Force


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         8/27/2025  11:15 PM                SecurityLogs
```



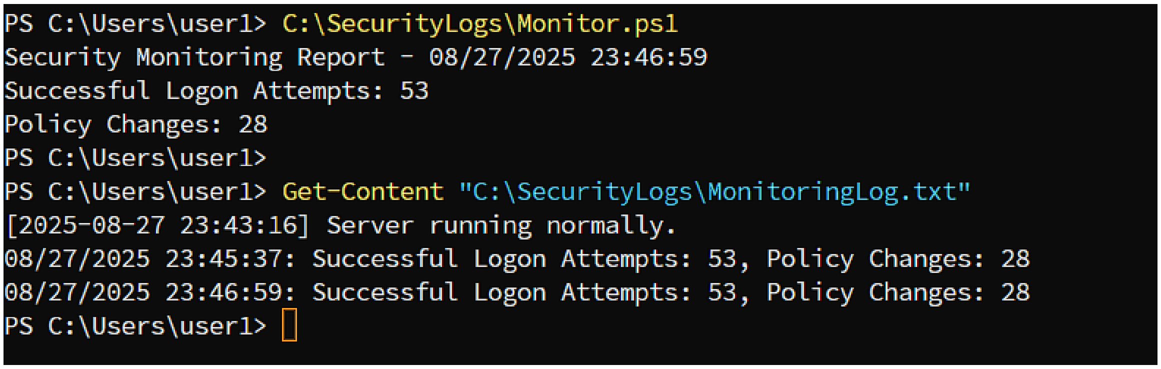
```
PS C:\Users\user1> New-Item -ItemType Directory -Path "C:\SecurityLogs" -Force


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         8/27/2025  11:15 PM                SecurityLogs


PS C:\Users\user1> $MonitorScript | Out-File -FilePath "C:\SecurityLogs\Monitor.ps1"
```

สร้าง Scheduled Task:



```
PS C:\Users\user1> $MonitorScript | Out-File -FilePath "C:\SecurityLogs\Monitor.ps1"
PS C:\Users\user1> $Action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "-ExecutionPolicy Bypass -File C:\SecurityLogs\Monitor.ps1"
PS C:\Users\user1> $Trigger = New-ScheduledTaskTrigger -Once -At (Get-Date) -RepetitionInterval (New-TimeSpan -Hours 1)
PS C:\Users\user1> $Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType ServiceAccount
PS C:\Users\user1> $Settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries -StartWhenAvailable
PS C:\Users\user1>
PS C:\Users\user1> Register-ScheduledTask -TaskName "SecurityMonitoring" -Action $Action -Trigger $Trigger -Principal $Principal -Settings $Settings

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\                                              SecurityMonitoring                Ready
```

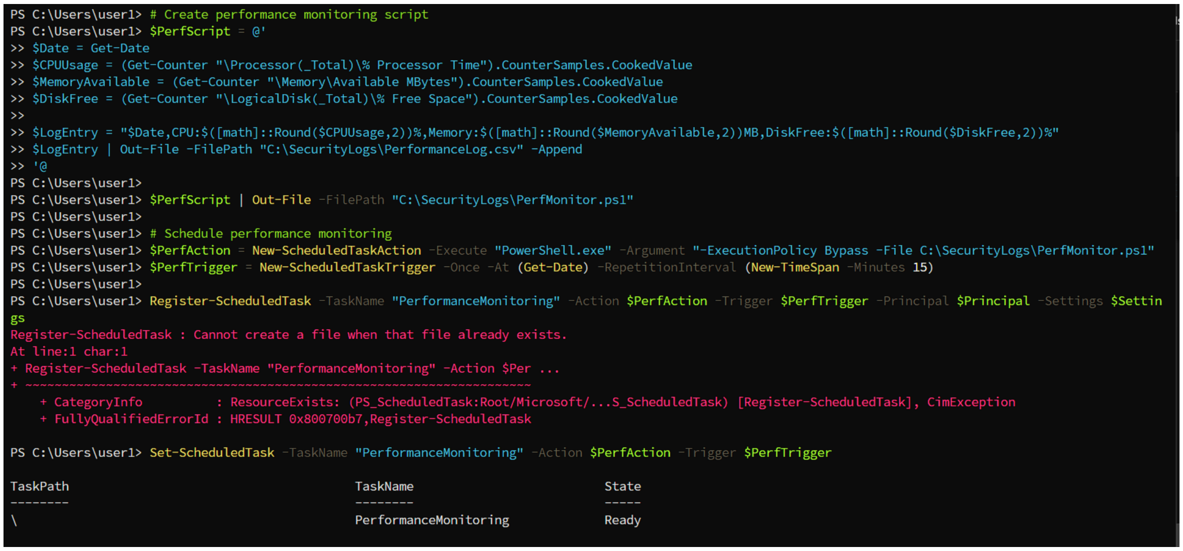
ไฟล์ Log MonitoringLog.txt



```
PS C:\Users\user1> C:\SecurityLogs\Monitor.ps1
Security Monitoring Report - 08/27/2025 23:46:59
Successful Logon Attempts: 53
Policy Changes: 28
PS C:\Users\user1>
PS C:\Users\user1> Get-Content "C:\SecurityLogs\MonitoringLog.txt"
[2025-08-27 23:43:16] Server running normally.
08/27/2025 23:45:37: Successful Logon Attempts: 53, Policy Changes: 28
08/27/2025 23:46:59: Successful Logon Attempts: 53, Policy Changes: 28
PS C:\Users\user1>
```

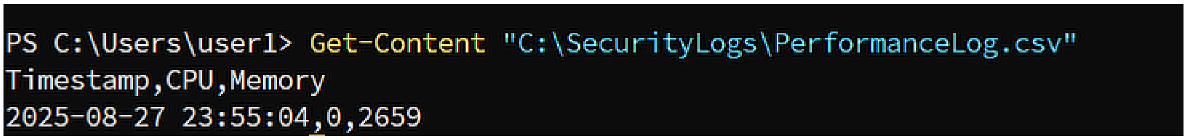
### Performance Monitoring

สร้างสคริปต์ Performance:



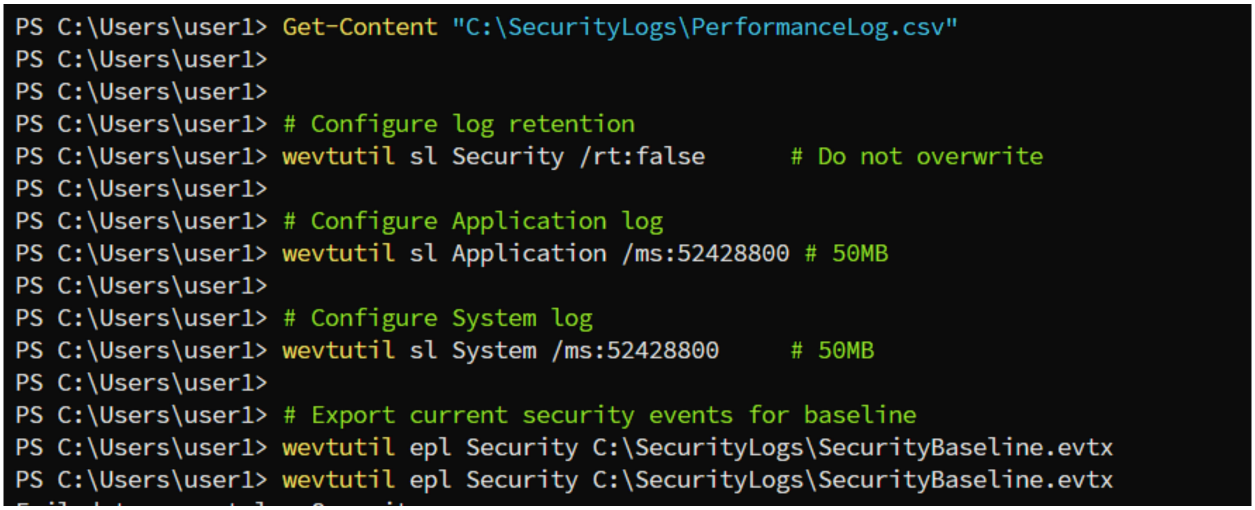
```
PS C:\Users\user1> # Create performance monitoring script
PS C:\Users\user1> $PerfScript = @'
>> $Date = Get-Date
>> $CPUUsage = (Get-Counter "\Processor(_Total)\% Processor Time").CounterSamples.CookedValue
>> $MemoryAvailable = (Get-Counter "\Memory\Available MBytes").CounterSamples.CookedValue
>> $DiskFree = (Get-Counter "\LogicalDisk(_Total)\% Free Space").CounterSamples.CookedValue
>>
>> $LogEntry = "$Date,CPU:$([math]::Round($CPUUsage,2))%,Memory:$([math]::Round($MemoryAvailable,2))MB,DiskFree:$([math]::Round($DiskFree,2))%"
>> $LogEntry | Out-File -FilePath "C:\SecurityLogs\PerformanceLog.csv" -Append
>> '@
PS C:\Users\user1>
PS C:\Users\user1> $PerfScript | Out-File -FilePath "C:\SecurityLogs\PerfMonitor.ps1"
PS C:\Users\user1>
PS C:\Users\user1> # Schedule performance monitoring
PS C:\Users\user1> $PerfAction = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "-ExecutionPolicy Bypass -File C:\SecurityLogs\PerfMonitor.ps1"
PS C:\Users\user1> $PerfTrigger = New-ScheduledTaskTrigger -Once -At (Get-Date) -RepetitionInterval (New-TimeSpan -Minutes 15)
PS C:\Users\user1>
PS C:\Users\user1> Register-ScheduledTask -TaskName "PerformanceMonitoring" -Action $PerfAction -Trigger $PerfTrigger -Principal $Principal -Settings $Settin
gs
Register-ScheduledTask : Cannot create a file when that file already exists.
At line:1 char:1
+ Register-ScheduledTask -TaskName "PerformanceMonitoring" -Action $Per ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceExists: (PS_ScheduledTask:Root/Microsoft/...S_ScheduledTask) [Register-ScheduledTask], CimException
    + FullyQualifiedErrorId : HRESULT 0x800700b7,Register-ScheduledTask

PS C:\Users\user1> Set-ScheduledTask -TaskName "PerformanceMonitoring" -Action $PerfAction -Trigger $PerfTrigger

TaskPath                                       TaskName                          State
--------                                       --------                          -----
\                                              PerformanceMonitoring             Ready
```

ไฟล Log PerformanceLog.csv



```
PS C:\Users\user1> Get-Content "C:\SecurityLogs\PerformanceLog.csv"
Timestamp,CPU,Memory
2025-08-27 23:55:04,0,2659
```

### Event Log Configuration



```
PS C:\Users\user1> Get-Content "C:\SecurityLogs\PerformanceLog.csv"
PS C:\Users\user1>
PS C:\Users\user1>
PS C:\Users\user1> # Configure log retention
PS C:\Users\user1> wevtutil sl Security /rt:false      # Do not overwrite
PS C:\Users\user1>
PS C:\Users\user1> # Configure Application log
PS C:\Users\user1> wevtutil sl Application /ms:52428800 # 50MB
PS C:\Users\user1>
PS C:\Users\user1> # Configure System log
PS C:\Users\user1> wevtutil sl System /ms:52428800     # 50MB
PS C:\Users\user1>
PS C:\Users\user1> # Export current security events for baseline
PS C:\Users\user1> wevtutil epl Security C:\SecurityLogs\SecurityBaseline.evtx
PS C:\Users\user1> wevtutil epl Security C:\SecurityLogs\SecurityBaseline.evtx
```

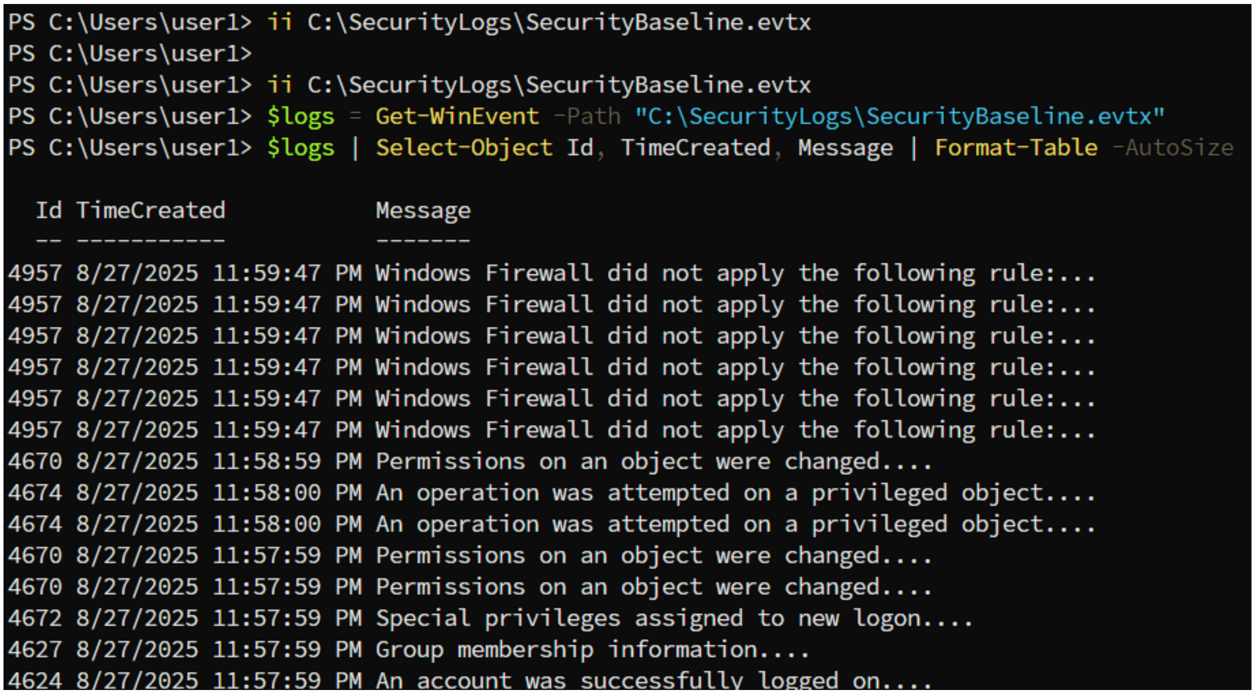
แสดง Event จาก SecurityBaseline.evtx เป็นตารางและสามารถ export เป็น CSV ได้

**1. Event ID** – ตัวเลขระบุชนิดเหตุการณ์ เช่น

- 4624 → Successful logon
- 4625 → Failed logon
- 4719 → Policy change
- 4740 → Account lockout
- 4672 → Special privileges

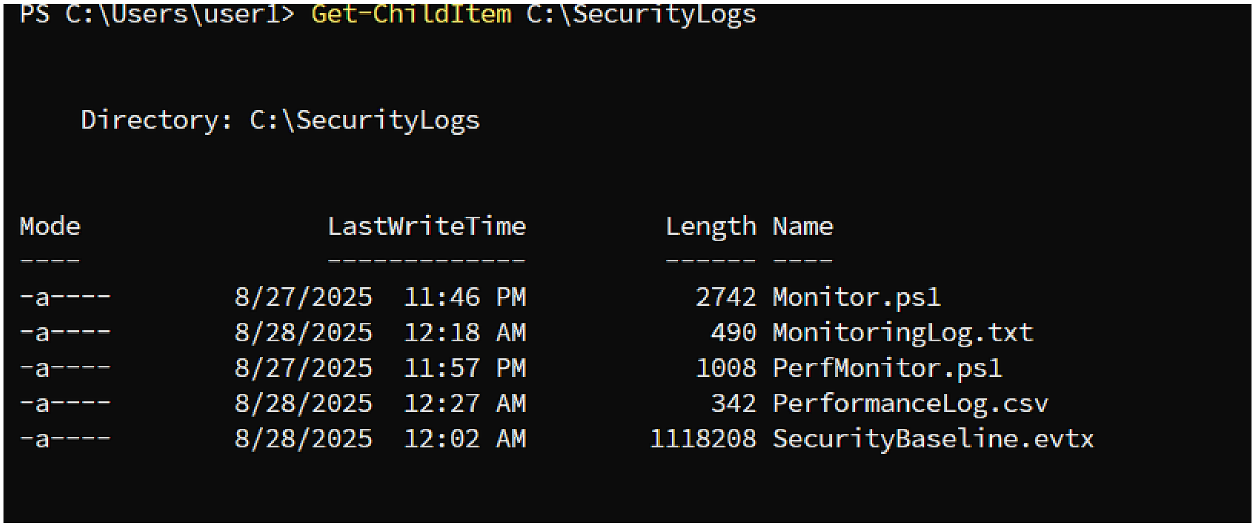
**2. TimeCreated** – เวลาที่เหตุการณ์เกิด

**3. Message** – รายละเอียดเหตุการณ์ทั้งหมด เช่น ชื่อผู้ใช้, SID, Computer, Logon Type, Failure Reason, Source IP (ถ้าเป็น remote logon)



```
PS C:\Users\user1> ii C:\SecurityLogs\SecurityBaseline.evtx
PS C:\Users\user1>
PS C:\Users\user1> ii C:\SecurityLogs\SecurityBaseline.evtx
PS C:\Users\user1> $logs = Get-WinEvent -Path "C:\SecurityLogs\SecurityBaseline.evtx"
PS C:\Users\user1> $logs | Select-Object Id, TimeCreated, Message | Format-Table -AutoSize

  Id TimeCreated           Message
  -- -----------           -------
4957 8/27/2025 11:59:47 PM Windows Firewall did not apply the following rule:...
4957 8/27/2025 11:59:47 PM Windows Firewall did not apply the following rule:...
4957 8/27/2025 11:59:47 PM Windows Firewall did not apply the following rule:...
4957 8/27/2025 11:59:47 PM Windows Firewall did not apply the following rule:...
4957 8/27/2025 11:59:47 PM Windows Firewall did not apply the following rule:...
4957 8/27/2025 11:59:47 PM Windows Firewall did not apply the following rule:...
4670 8/27/2025 11:58:59 PM Permissions on an object were changed....
4674 8/27/2025 11:58:00 PM An operation was attempted on a privileged object....
4674 8/27/2025 11:58:00 PM An operation was attempted on a privileged object....
4670 8/27/2025 11:57:59 PM Permissions on an object were changed....
4670 8/27/2025 11:57:59 PM Permissions on an object were changed....
4672 8/27/2025 11:57:59 PM Special privileges assigned to new logon....
4627 8/27/2025 11:57:59 PM Group membership information....
4624 8/27/2025 11:57:59 PM An account was successfully logged on....
```

ไฟล์ที่อยู่ใน โฟลเดอร์ SecurityLogs



```
PS C:\Users\user1> Get-ChildItem C:\SecurityLogs


    Directory: C:\SecurityLogs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/27/2025  11:46 PM           2742 Monitor.ps1
-a----         8/28/2025  12:18 AM            490 MonitoringLog.txt
-a----         8/27/2025  11:57 PM           1008 PerfMonitor.ps1
-a----         8/28/2025  12:27 AM            342 PerformanceLog.csv
-a----         8/28/2025  12:02 AM        1118208 SecurityBaseline.evtx
```