**Tạo file domain.ps1**

<https://www.dropbox.com/s/4y907djrvtf6hxk/domain.ps1?dl=1>

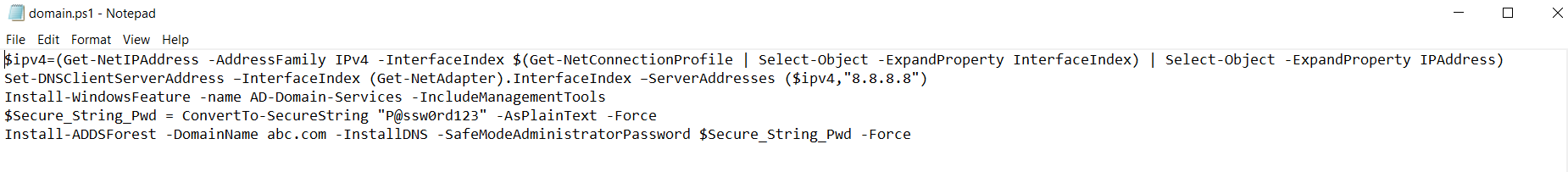
$ipv4=(Get-NetIPAddress -AddressFamily IPv4 -InterfaceIndex $(Get-NetConnectionProfile | Select-Object -ExpandProperty InterfaceIndex) | Select-Object -ExpandProperty IPAddress)

Set-DNSClientServerAddress –InterfaceIndex (Get-NetAdapter).InterfaceIndex –ServerAddresses ($ipv4,"8.8.8.8")

Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools

$Secure\_String\_Pwd = ConvertTo-SecureString "P@ssw0rd123" -AsPlainText -Force

Install-ADDSForest -DomainName abc.com -InstallDNS -SafeModeAdministratorPassword $Secure\_String\_Pwd -Force



**Tạo file dowload.ps1**

$Url="<https://www.dropbox.com/s/4y907djrvtf6hxk/domain.ps1?dl=1>"

Invoke-WebRequest $Url -OutFile c:\domain.ps1

$Url1="https://www.dropbox.com/s/15o7vin7fps2ol5/remove.ps1?dl=1"

Invoke-WebRequest $Url1 -OutFile c:\remove.ps1

**Remove.ps1**

Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name 'NV Domain' -Value '0'

Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name 'Domain' -Value '0'

Restart-Computer

**3, Thực thi code**

class test{

exec{'file':

path => 'C:/Windows/System32/WindowsPowerShell/v1.0',

command => 'powershell curl https://tinyurl.com/y4pd6emm -O download.ps1',

}

exec {'download\_file':

path => 'C:/Windows/System32/WindowsPowerShell/v1.0',

command => 'powershell -executionpolicy remotesigned -file C:/download.ps1',

}

exec {'excute\_file':

path => 'C:/Windows/System32/WindowsPowerShell/v1.0',

command => 'powershell -executionpolicy remotesigned -file C:/domain.ps1',

}

}

class remove{

exec {'remove\_domain':

path => 'C:/Windows/System32/WindowsPowerShell/v1.0',

command => 'powershell -executionpolicy remotesigned -file C:/remove.ps1',

}

}

class remove\_file{

exec {'remove1':

path => 'C:/Windows/System32/WindowsPowerShell/v1.0',

command => 'powershell Remove-item download.ps1',

}

exec {'remove2':

path => 'C:/Windows/System32/WindowsPowerShell/v1.0',

command => 'powershell Remove-item domain.ps1',

}

}

if $facts['os']['family'] == 'windows'{

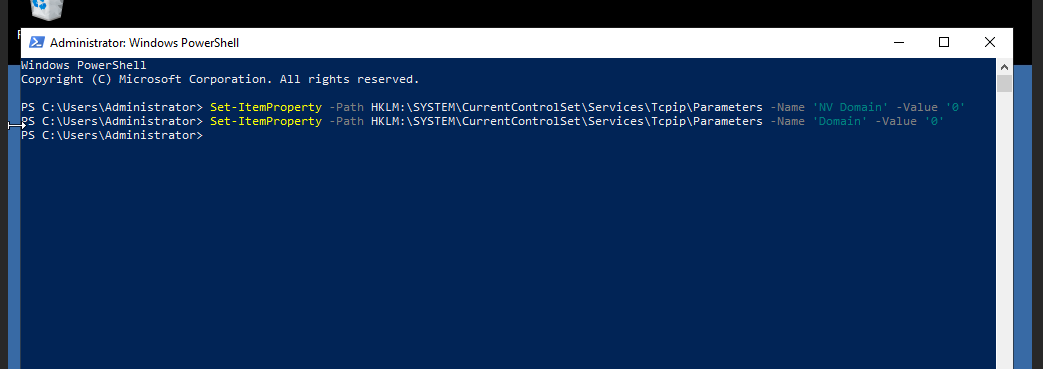
include test

include remove\_file

}



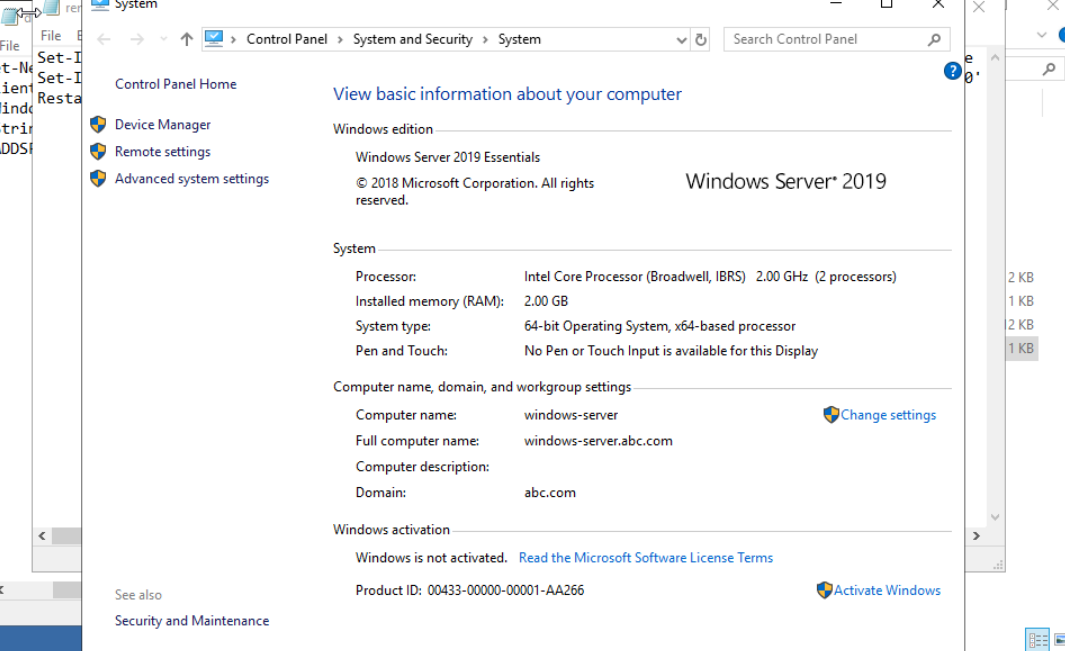
3, Xóa domain



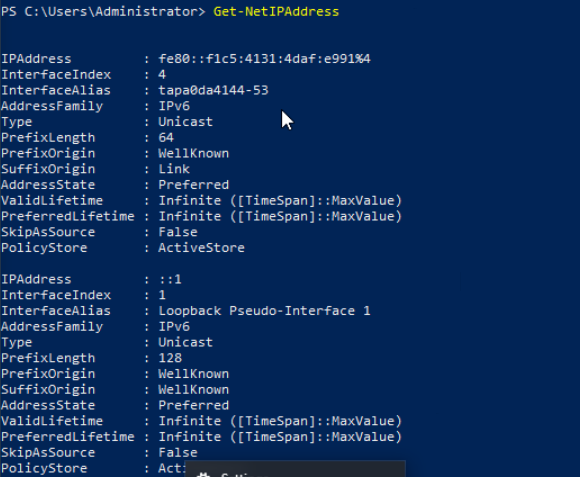
if $facts['os']['family'] == 'windows'{

include remove

}



Check qua client



Lấy card mạng máy client

-Chỉnh DNS Server thành ip của server win2019:

-Tham gia vào domain:



Máy sẽ tự động khởi động lại và máy client đã tham gia vào domain abc.com

