

# Forum:[Hack Forums](#)

Thread: [PowerShell Remote WMI Query Tool](#)

Travelers - July 27, 2017, 3:02 pm

It has been awhile since I posted anything in this section and I wanted to share my latest script. A buddy at work and I put this together because we needed to be able to query remote services on non-domain servers. This could be a good learning tool for those still new to PS.

What do you guys think? It has no error control, so type carefully.

```
Code #The name of the machine
$Name = Read-Host 'What Machine do you want to connect to? (Note: Name Must contain no
spaces and be exact)'
Read-Host 'Please enter a credintial Domain\User (Note: Passwords are stored and sent
encrypted)'
$C = Get-Credential
#This returns all the services on a server:
$service = Get-WmiObject -Class Win32_Service -Impersonation 3 -Credential $C -ComputerName
$Name | Format-Table Name, DisplayName, State, StartMode, StartName
#Select a Service
$service
$ServiceName = Read-Host 'Please Enter a service Name'
$service = Get-WmiObject -Class Win32_Service -Filter "Name = '$ServiceName'" -Impersonation
3 -Credential $C -ComputerName $Name
#Options Var
While(($State = Read-Host -Prompt "Select a command") -ne "5"){
switch($State){
    1 {"Start Service"}
    2 {"Stop Service"}
    3 {"Restart Service"}
    4 {"Status"}
    5 {"Exit"}
    default {"Invalid entry"}
}
    if ( $State -eq 1)
    {
        $service.StartService()
        $service
    }
    elseif ( $State -eq 2)
    {
        $service.StopService()
        $service
    }
    elseif ( $State -eq 3)
    {
        $service.Stopservice()
        $service.StartService()
        $service
    }
}
```

```
}  
elseif ( $State -eq 4)  
{  
    $service  
}  
}
```