**ePortfolio Link:** [**https://github.com/DilshaWe/ePortfolio.git**](https://github.com/DilshaWe/ePortfolio.git)

**Assignment 2 : Task 1 PowerShell**

Q1. List any processes that are hogging the CPU. Provide an explanation of your test in your code’s documentation. Submit an example run of your script detecting a CPU hogging process.

function CpuHoggings {

Get-Process | Sort-Object -property CPU -descending | Select-Object -first 5

}

CpuHoggings (5)

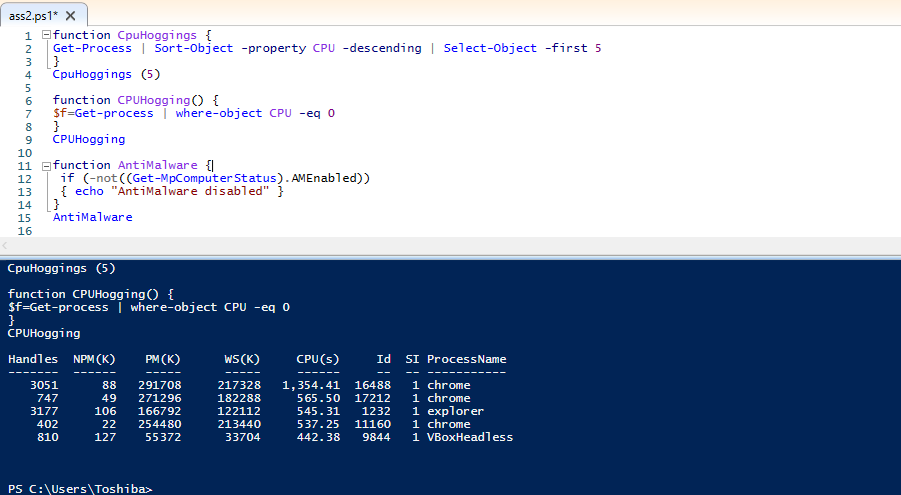
or

function CPUHogging() {

$f=Get-process | where-object CPU -eq 0

}

CPUHogging



Q2. Check that Windows Defender antimalware toolkit is enabled.

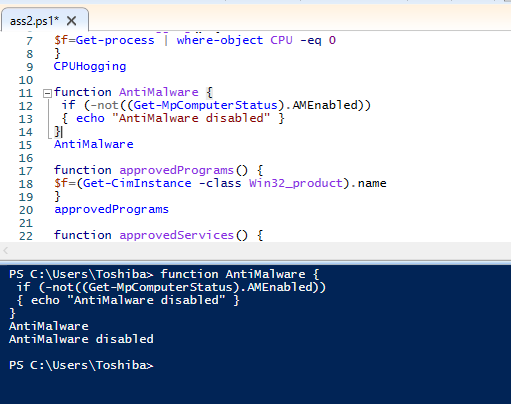
function AntiMalware {

if (-not((Get-MpComputerStatus).AMEnabled))

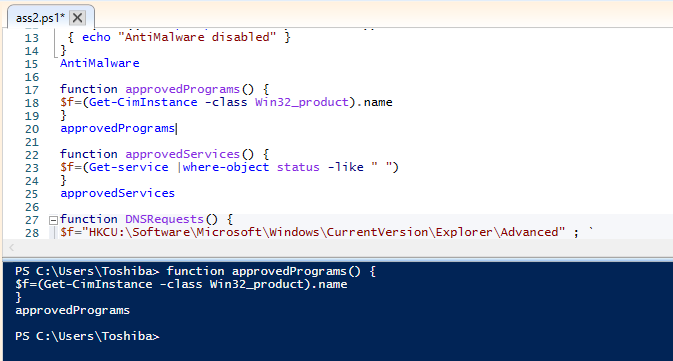
{ echo "AntiMalware disabled" }

}

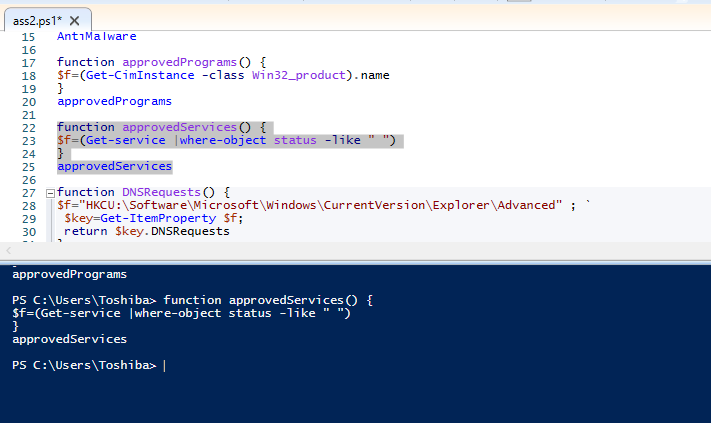
AntiMalware



3. Create a software inventory that is a list of approved programs. Check that only approved programs are installed. Submit your list of approved programs. Remove one of the approved programs from your list. Submit an example run of your script detecting an unapproved program

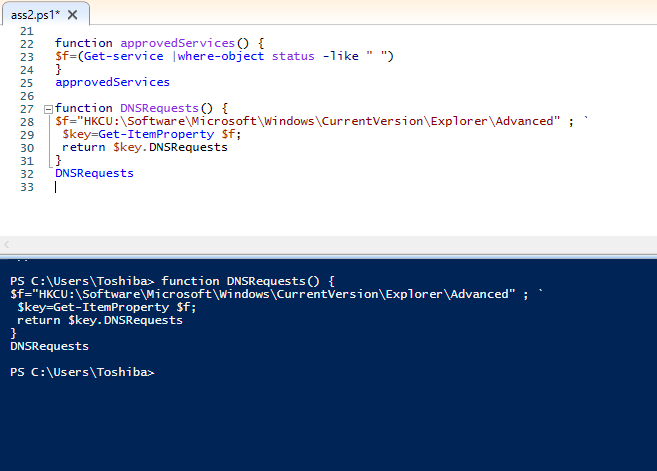


4. Create a list of services approved for running. Check that only approved services are running. Remove one of the approved services from your list. Submit an example run of your script detecting an unapproved service.

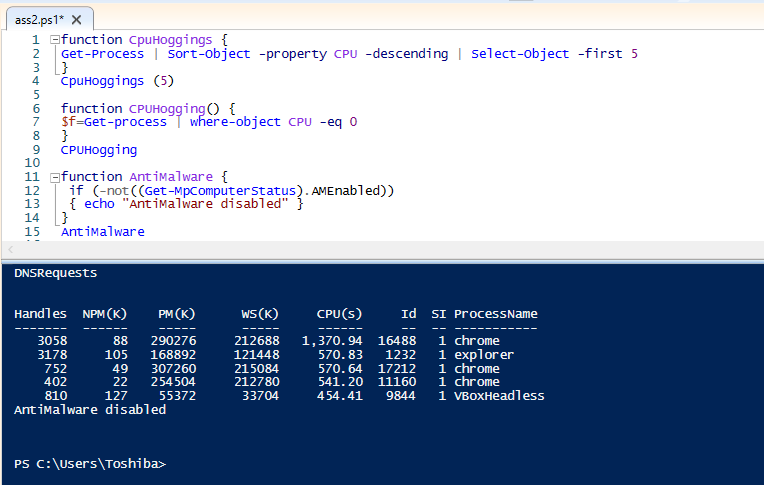


5. Please implement one of the following three tasks: either part a, part b or part c. You do not need to implement all of part a, b and c.

b. Check Cortana has been disabled on the Windows PC. That is, ensure that HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Search\AllowCortana is set to 0.



6. Check the script is running under your hardcoded username.



* End of the submission -