Patching Windows On A Dedicated Server For WannaCry SMB Attack

Introduction

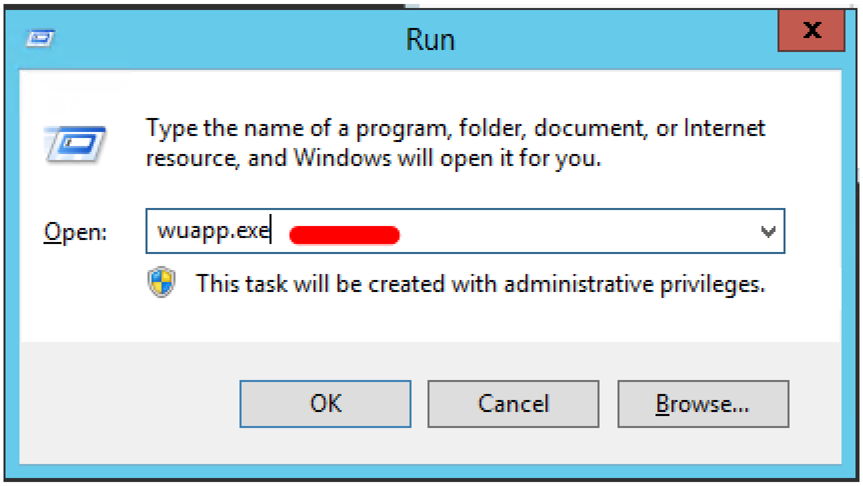
This document list down the steps you need to take to update/patch your windows OS.

Here we will demonstrate how to update windows using GUI and CUI. Although both the methods are doing the same thing, we recommend that you should use GUI as there are very little chances of error and it is easy to troubleshoot in case of issues.

Using GUI

Below are the steps you need to take in order to update/patch your windows using graphical user interface.

Step 1: Open the windows update control panel. To open the same go to Start>Type"windows update">Enter or Start>Run>Type"wuapp.exe" in the run window and press enter.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wuapp.exe

This task will be created with administrative privileges.

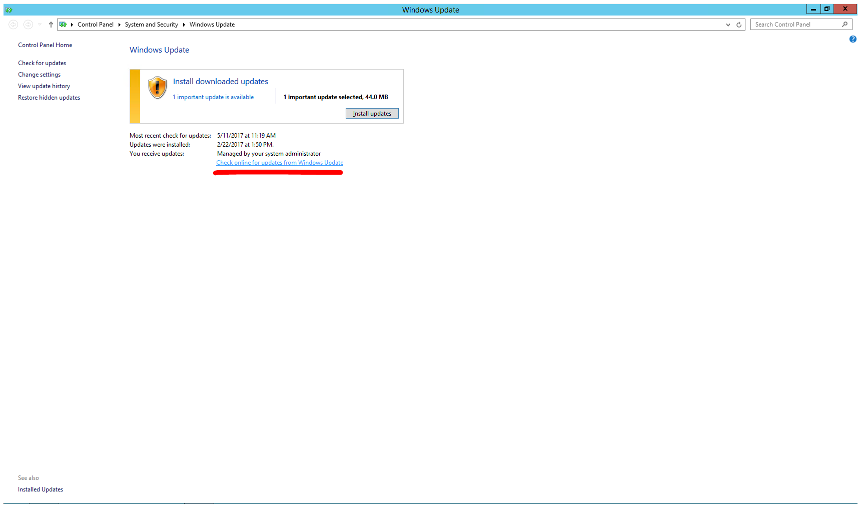
Step 2:

A. Click on "Check online for updates from Windows Update". or

B. "Check for updates" whichever is available from A and B.

C. If the automatic updating is not enabled in windows update setting then it will give an error, if it is the case then click on "Turn on automatic updates".

A.



Windows Update

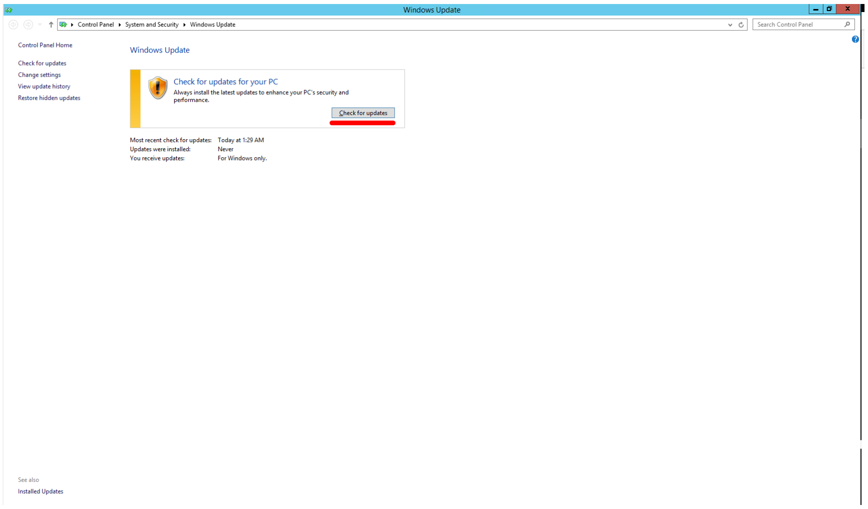
Install downloaded updates

1 important update is available

1 important update selected, 44.0 MB

Most recent check for updates: 5/11/2017 at 11:19 AM
Updates were installed: 2/22/2017 at 1:50 PM.
You receive updates: Managed by your system administrator
Check online for updates from Windows Update

B.



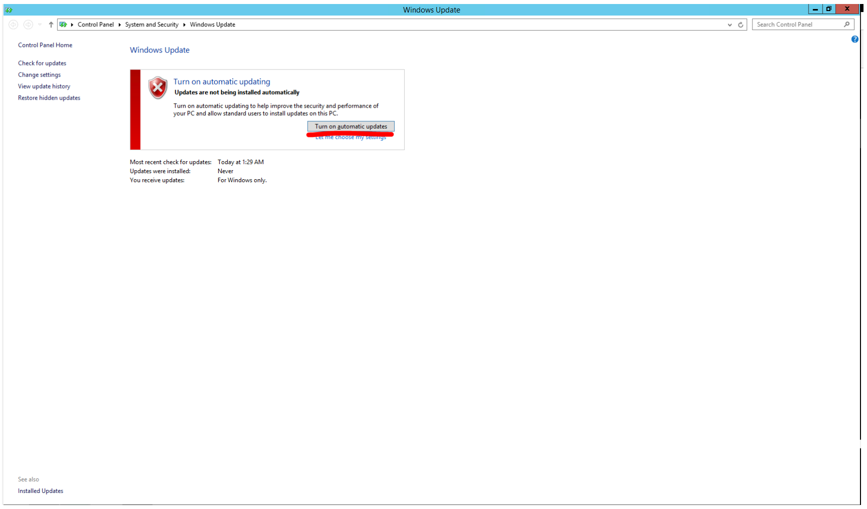
Windows Update

Check for updates for your PC

Always install the latest updates to enhance your PC's security and performance.

Most recent check for updates: Today at 1:29 AM
Updates were installed: Never
You receive updates: For Windows only.

C.



Windows Update

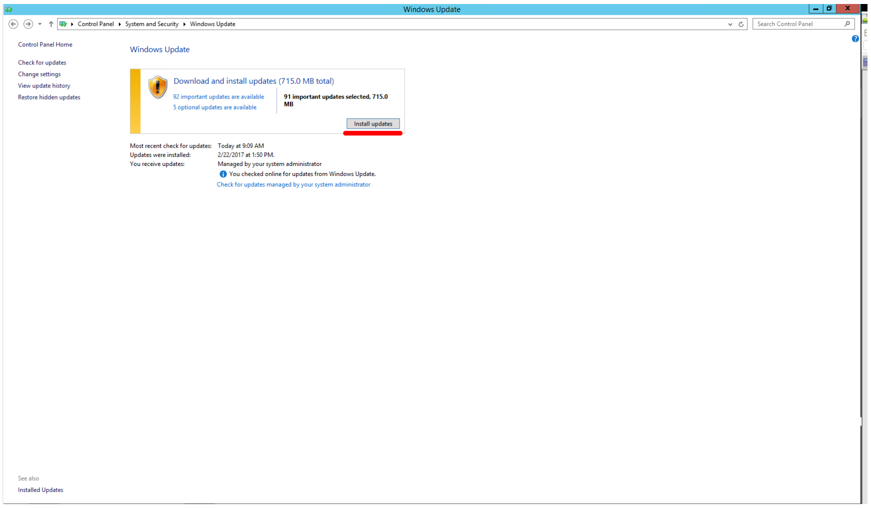
Turn on automatic updating

Updates are not being installed automatically

Turn on automatic updating to help improve the security and performance of your PC and allow standard users to install updates on this PC.

Most recent check for updates: Today at 1:29 AM
Updates were installed: Never
You receive updates: For Windows only.

Step 3: Select all important updates and click on "Install Updates"



Windows Update

Download and install updates (715.0 MB total)

92 important updates are available

5 optional updates are available

91 important updates selected, 715.0 MB

Most recent check for updates: Today at 9:09 AM

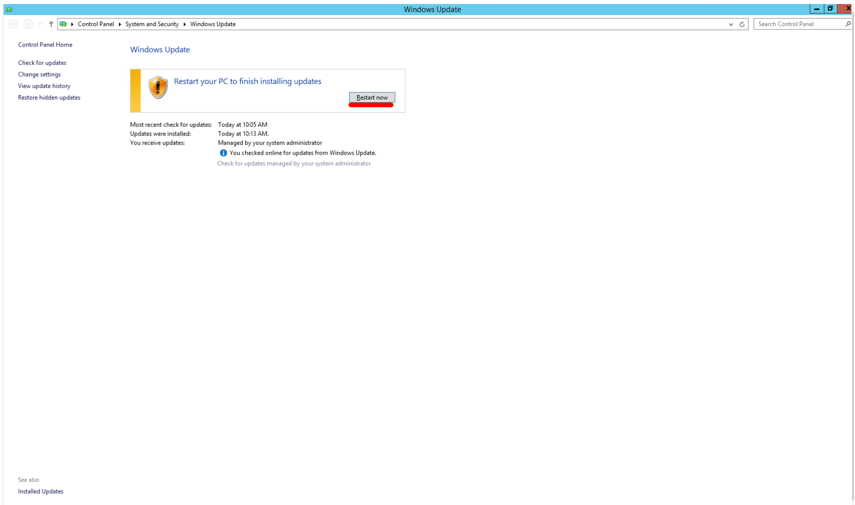
Updates were installed: 2/22/2017 at 1:50 PM.

You receive updates: Managed by your system administrator

You checked online for updates from Windows Update.

Check for updates managed by your system administrator

Step 4: As soon as the installation is finished, click on "Restart now" to reboot the server.



Windows Update

Restart your PC to finish installing updates

Most recent check for updates: Today at 10:05 AM

Updates were installed: Today at 10:13 AM.

You receive updates: Managed by your system administrator

You checked online for updates from Windows Update.

Check for updates managed by your system administrator

Step 5:

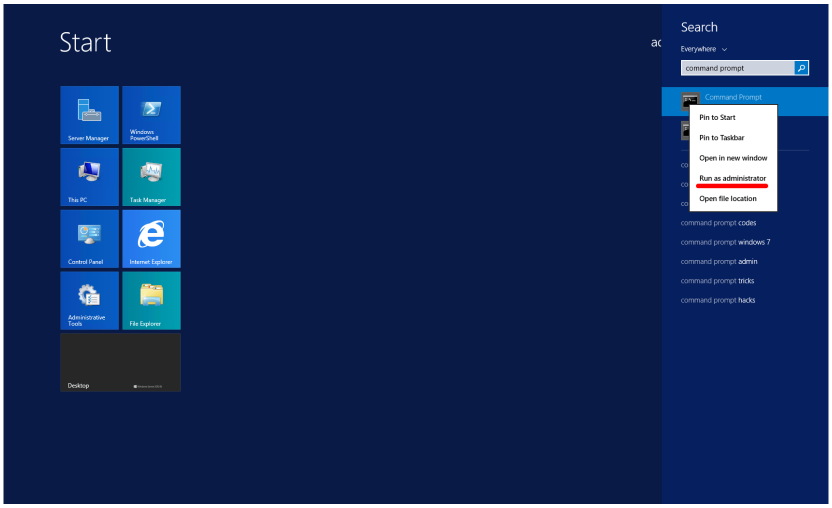
After the reboot start over with the step 1 to ensure that there are no pending updates.

Using CUI

Below are the steps you need to take in order to update/patch your windows using Command line interface.

Method 1: Using Native Commands

Step 1: Start a command prompt window as administrator. To do the same, go to Start>Type"Command Prompt">Right Click on Command Prompt>

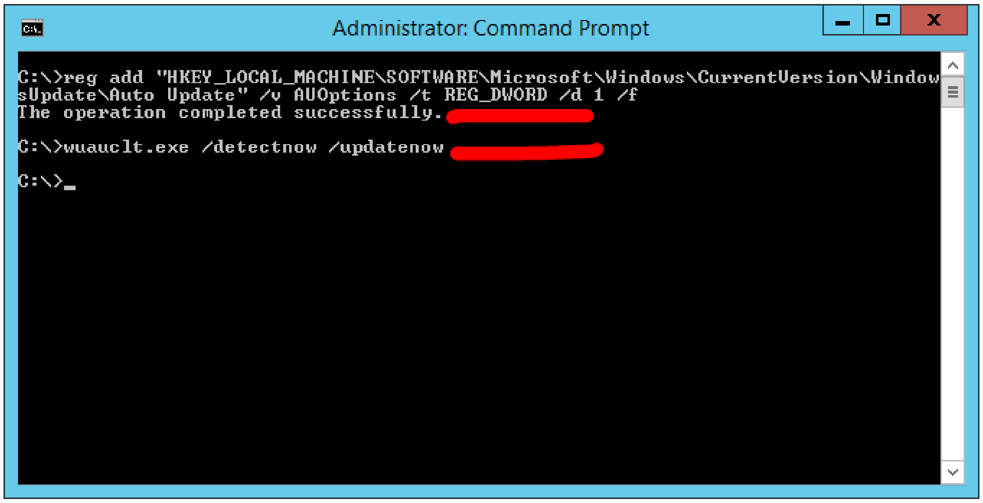


Step 2: To check and update the windows type the below command and press enter.

Command:

1. reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 1 /f
2. wuauclt.exe /detectnow /updatenow

Note: This will not work if you have set "Never check for updates" in Windows Update settings. In this case go for GUI option given above.



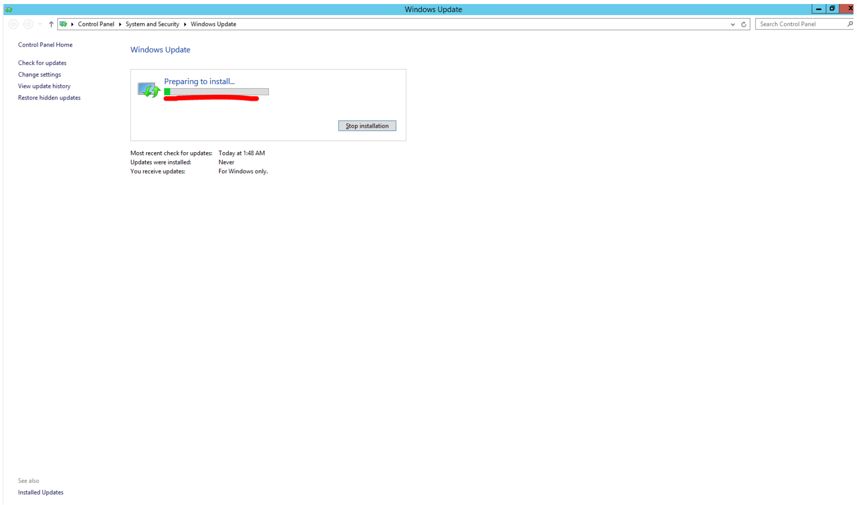
```
C:\>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Window
sUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 1 /f
The operation completed successfully.

C:\>wuauclt.exe /detectnow /updatenow

C:\>_
```

Step 3: After running the same when you open the windows update control panel, you will be able to see the status of the installation.

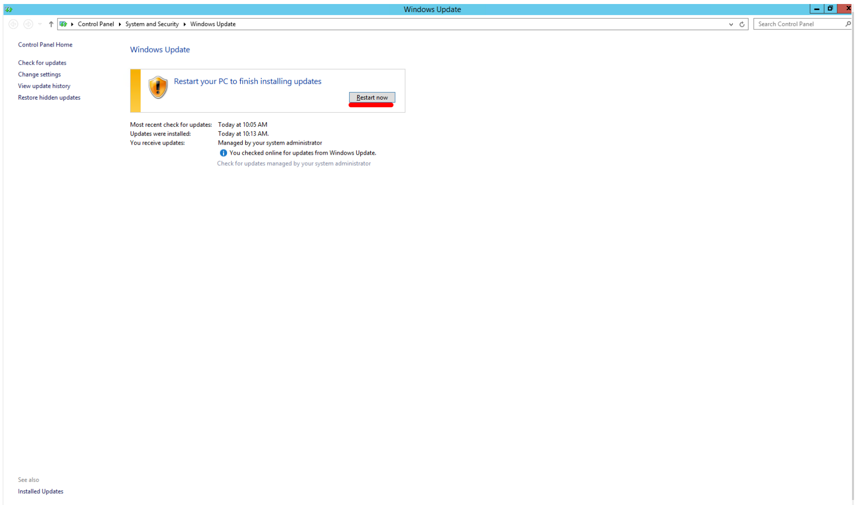
Note: You will be able to see the status after at least 5-10 minutes of running the command as it will detect the updates first then it will start preparing to install the updates. If the status is not being shown then it is better to go for GUI option. Although you can check the status in the following log if you want to troubleshoot: C:\Windows\WindowsUpdate.log



Preparing to install...

Most recent check for updates: Today at 1:48 AM
Updates were installed: Never
You receive updates: For Windows only.

Step 4: Once the installation is finished, reboot the server by clicking on "Restart now"



Restart your PC to finish installing updates

Most recent check for updates: Today at 10:05 AM
Updates were installed: Today at 10:13 AM.
You receive updates: Managed by your system administrator
You checked online for updates from Windows Update.
Check for updates managed by your system administrator

Step 5:

After the reboot start over with the step 1 to ensure that there are no pending updates.

Method 2:Using VB Script

To update windows using a VB script provided by Microsoft in the below link you have to follow the instructions provided in the link itself.

Note: We have tested the same on our test server and the script works seamlessly. You might have to enable automatic updating using below command before running the script

reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 1 /f

https://msdn.microsoft.com/en-us/library/aa387102(v=vs.85).aspx

Verification Steps For SMB Attack Vulnerability After The Update

Verify on Windows 2008 R2

There are two patches released by Microsoft for Windows 2008 R2 as per the following doc.

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

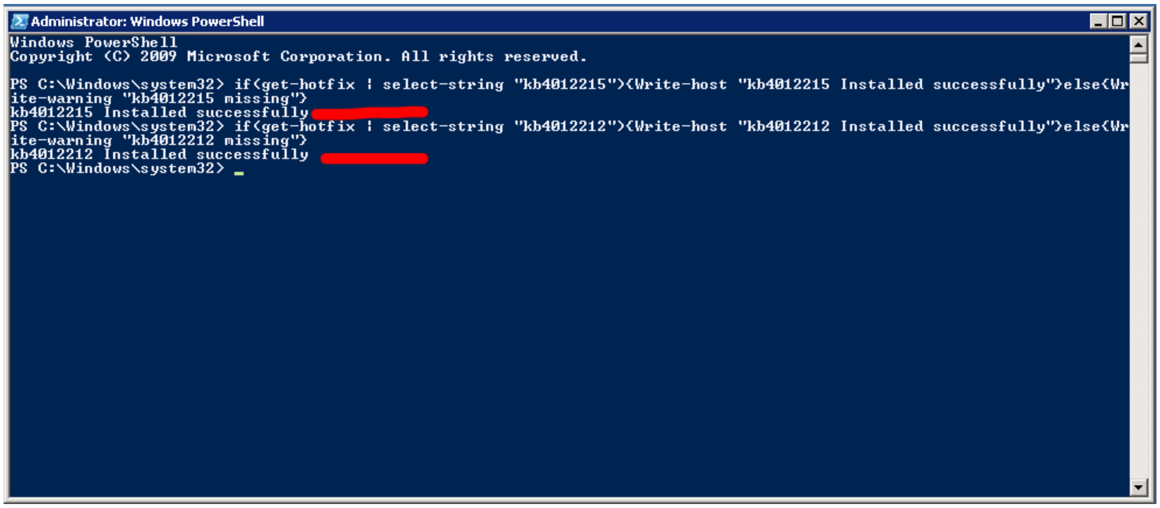
1. KB4012215

2. KB4012212

Open Powershell window as Administrator and run below command:

if(get-hotfix | select-string "kb4012215"){Write-host "kb4012215 Installed successfully"}else{Write-warning "kb4012215 missing"}
if(get-hotfix | select-string "kb4012212"){Write-host "kb4012212 Installed successfully"}else{Write-warning "kb4012212 missing"}

The output will tell you if the server is patched properly or the update is missing.



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> if(get-hotfix | select-string "kb4012215"){Write-host "kb4012215 Installed successfully"}else{Wr
ite-warning "kb4012215 missing"}
kb4012215 Installed successfully
PS C:\Windows\system32> if(get-hotfix | select-string "kb4012212"){Write-host "kb4012212 Installed successfully"}else{Wr
ite-warning "kb4012212 missing"}
kb4012212 Installed successfully
PS C:\Windows\system32> _
```

Verify on Windows 2012 R2

There are two patches released by Microsoft for Windows 2012 R2 as per the following doc.

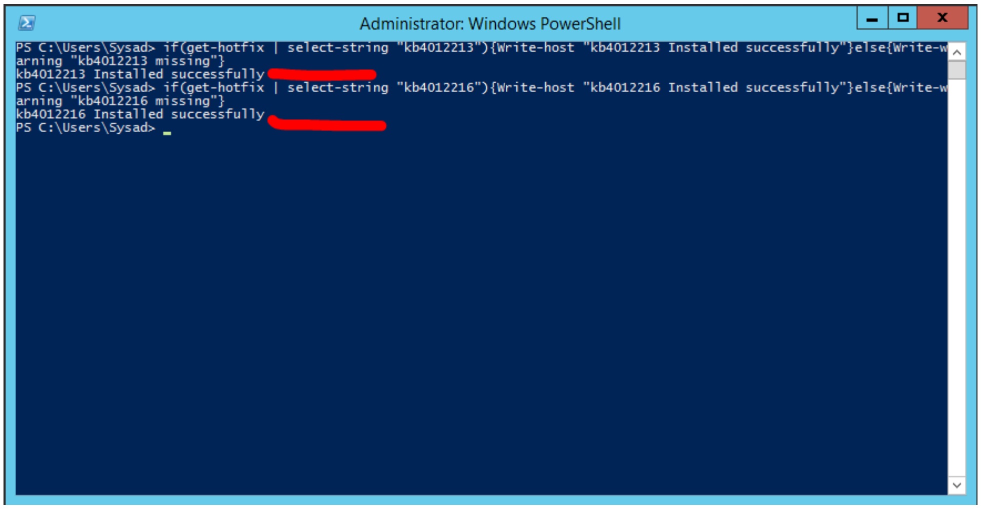
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

1. KB4012213
2. KB4012216

Open Powershell window as Administrator and run below command:

if(get-hotfix | select-string "kb4012213"){Write-host "kb4012213 Installed successfully"}else{Write-warning "kb4012213 missing"}
if(get-hotfix | select-string "kb4012216"){Write-host "kb4012216 Installed successfully"}else{Write-warning "kb4012216 missing"}

The output will tell you if the server is patched properly or the update is missing.



```
PS C:\Users\Sysad> if(get-hotfix | select-string "kb4012213"){Write-host "kb4012213 Installed successfully"}else{Write-w
arning "kb4012213 missing"}
kb4012213 Installed successfully
PS C:\Users\Sysad> if(get-hotfix | select-string "kb4012216"){Write-host "kb4012216 Installed successfully"}else{Write-w
arning "kb4012216 missing"}
kb4012216 Installed successfully
PS C:\Users\Sysad> _
```

References

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx https://msdn.microsoft.com/en-us/library/aa387102(v=vs.85).aspx