

Patching Windows On A Dedicated Server

- Introduction
- Using GUI
- Using CUI
 - Method 1: Using Native Commands
 - Method 2: Using VB Script
- Verification Steps For SMB Attack Vulnerability After The Update
 - Verify on Windows 2008 R2
 - Verify on Windows 2012 R2
- References

Introduction

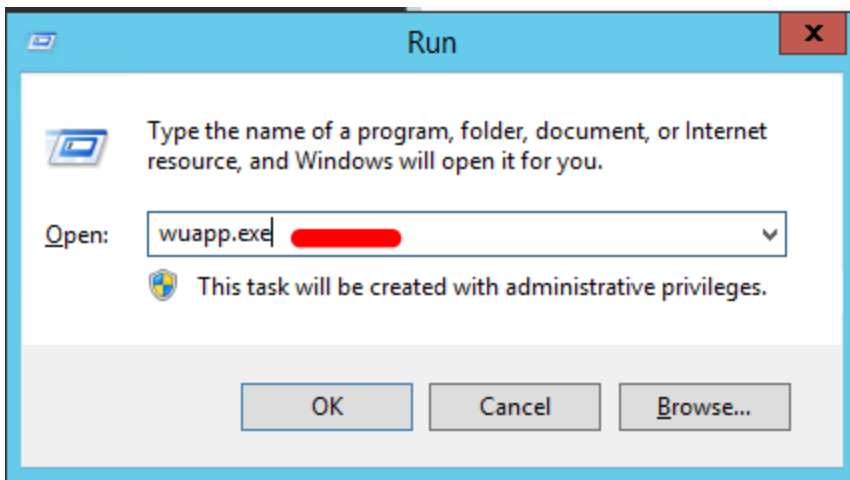
This document lists down the steps you need to take to update/patch your windows OS.

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.



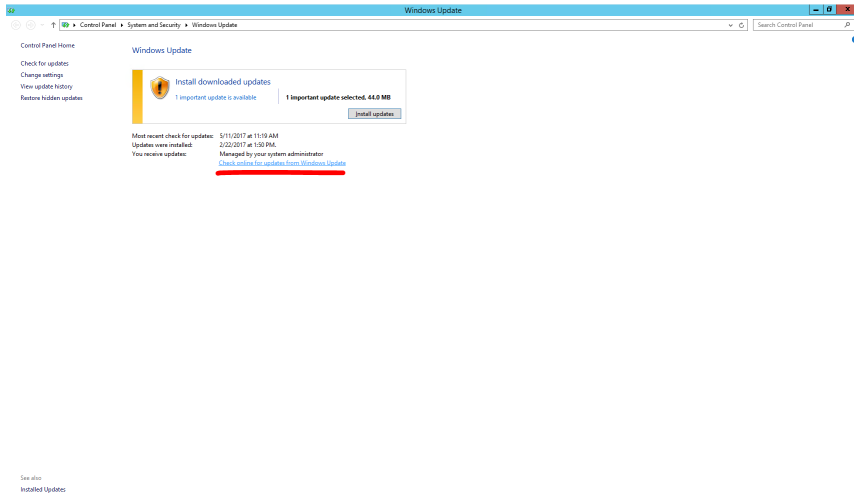
Step 2:

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

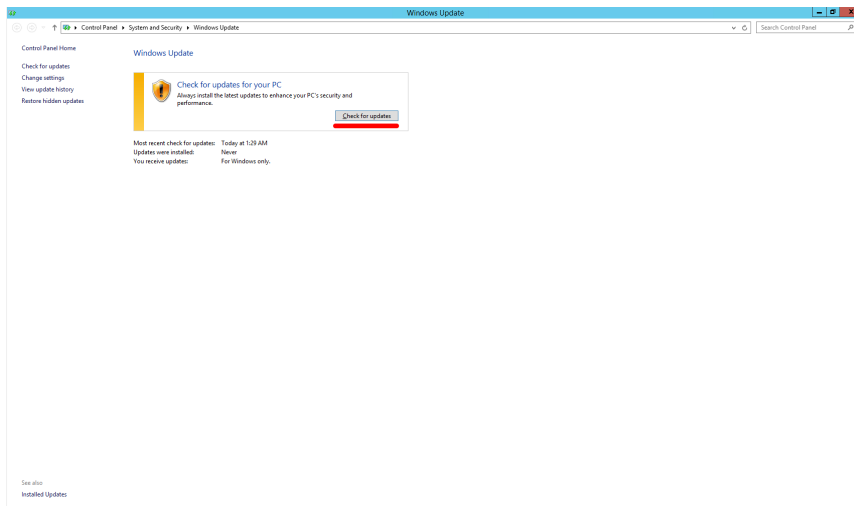
B. "Check for updates" whichever is available from A and B.

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".

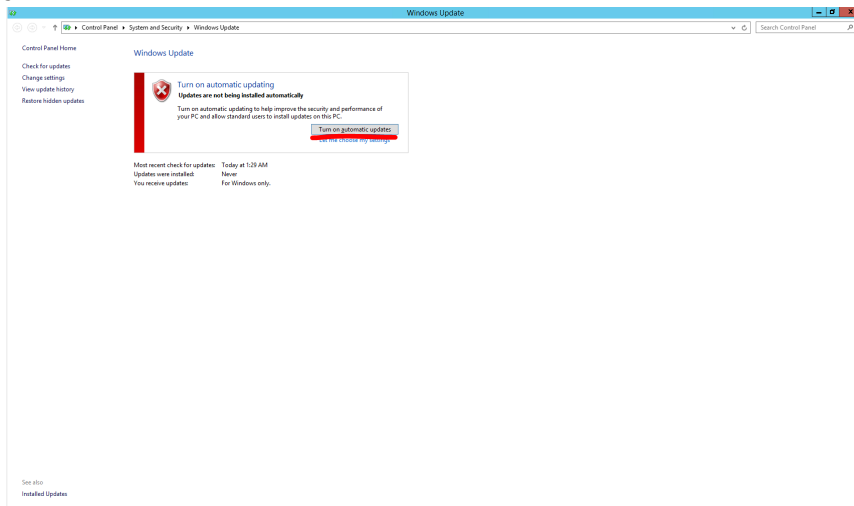
A.



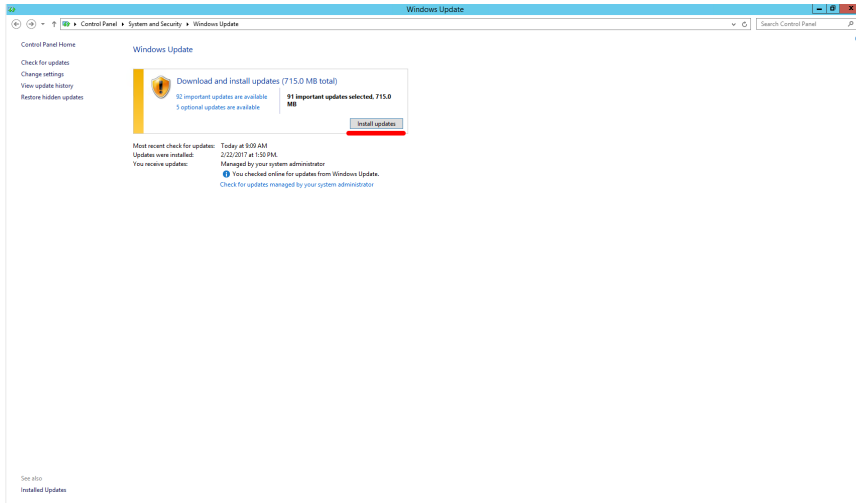
B.



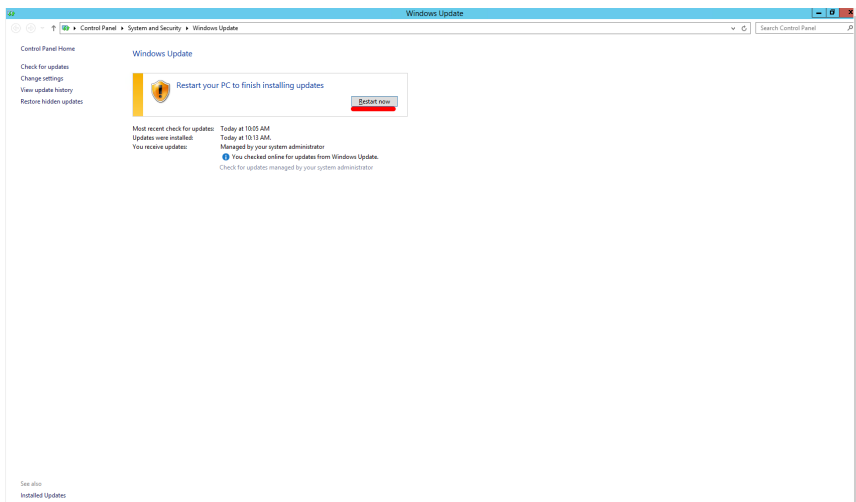
C.



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



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

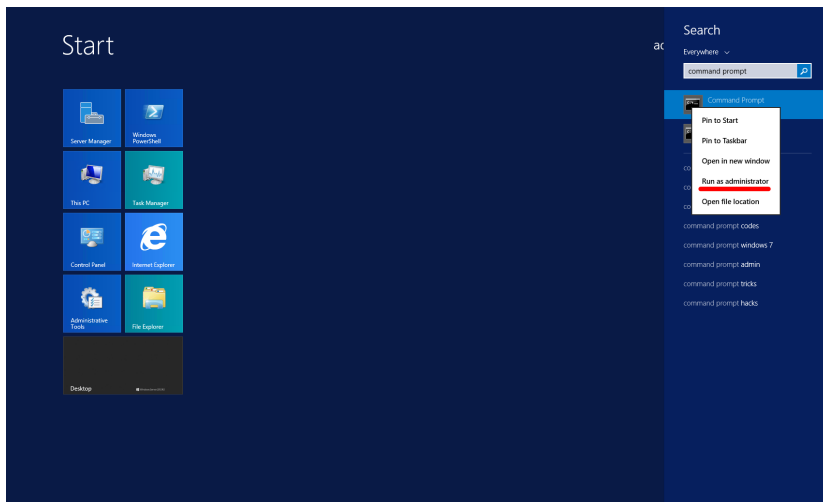


Using CUI

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>

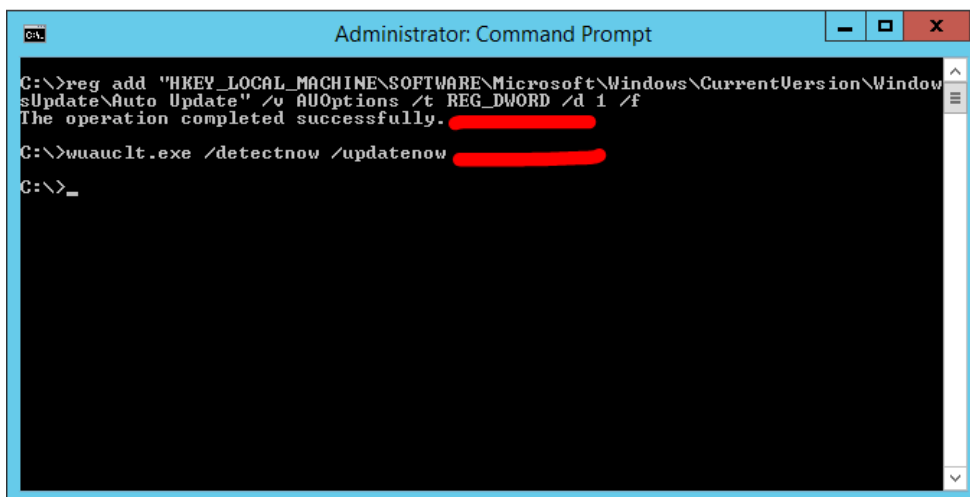


Step 2: To check and update the windows type the below command and press enter.

Command:

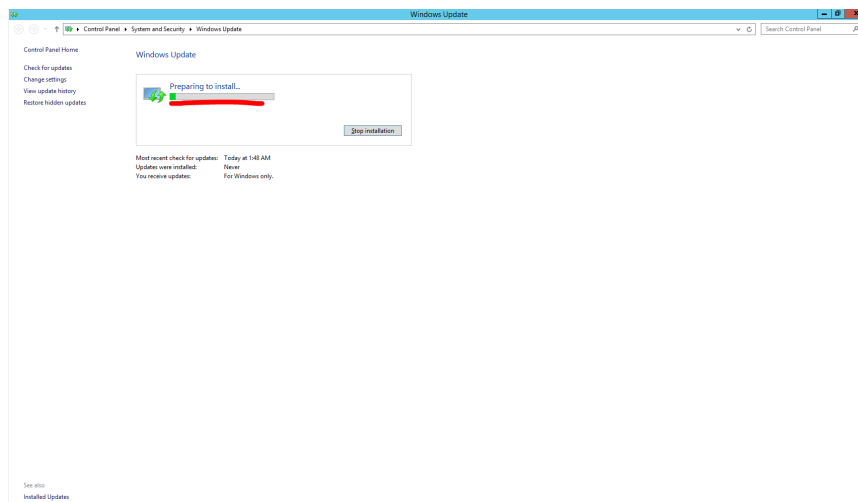
1. `reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 1 /f`
2. `wuauclt.exe /detectnow /updatenow`

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.

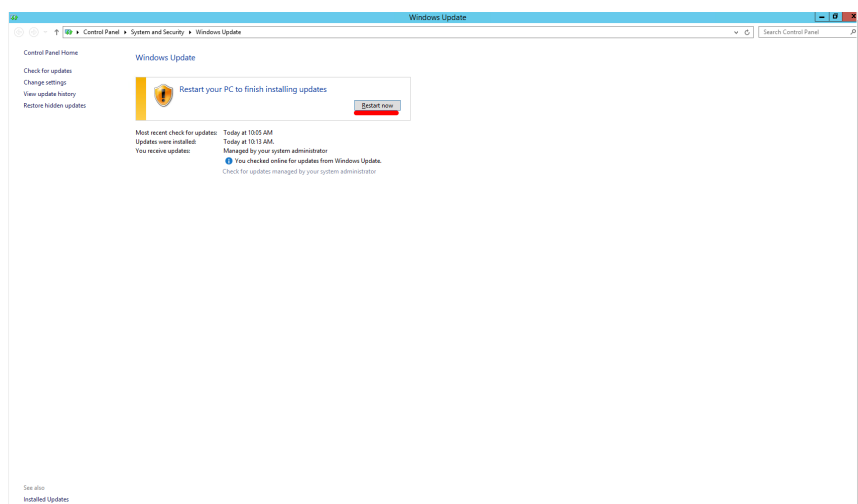


Step 3: After running the same when you open the windows update control panel, you will be able to see the status of the installation.

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`



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



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](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.

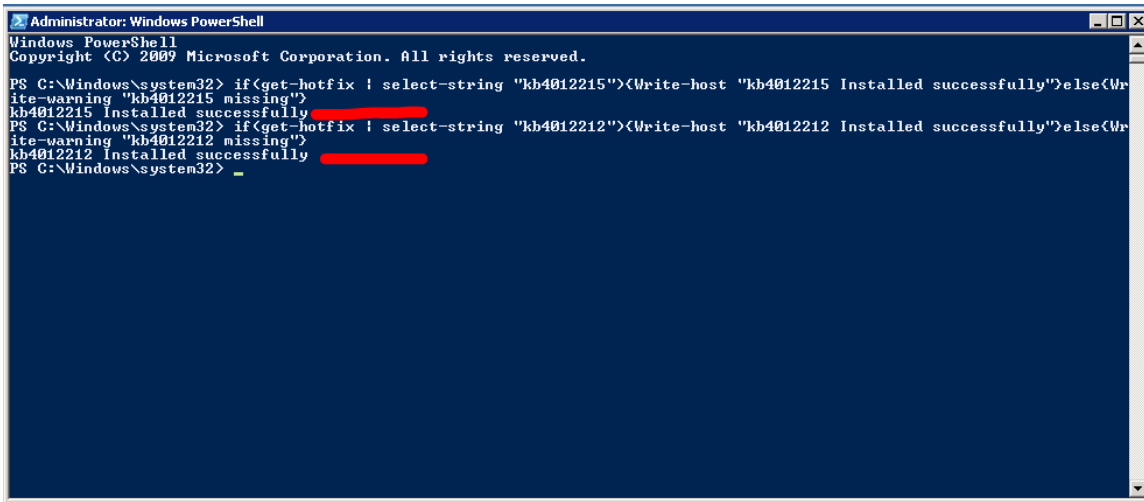
<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

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.



Verify on Windows 2012 R2

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

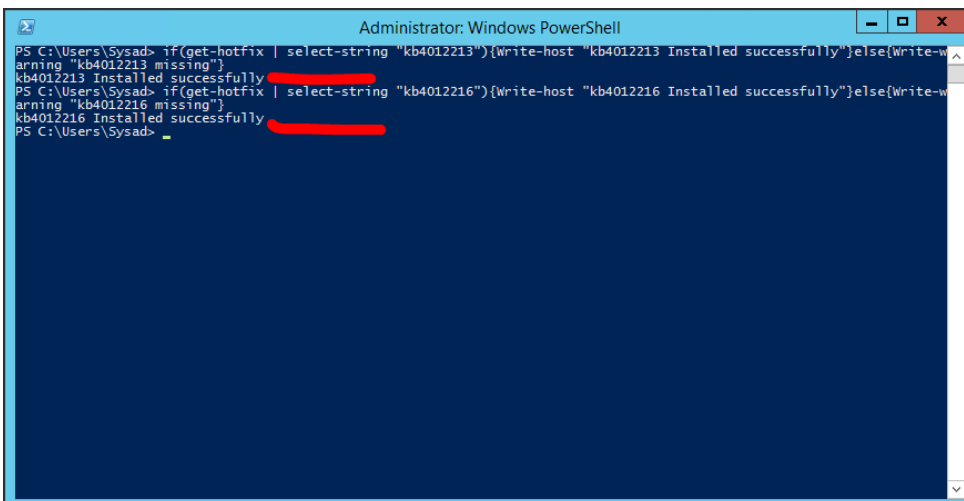
<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

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.



References

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

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

