A · P · U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

ASSIGNMENT

TECHNOLOGY PARK MALAYSIA

AICT006-4-2-DSF

DIGITAL SECURITY AND FORENSICS

UCDF2104ICT (SE)

HAND OUT DATE: 12 DECEMBER 2022

HAND IN DATE: 19 MARCH 2023

WEIGHTAGE: 20%

INSTRUCTIONS TO CANDIDATES:

1 Submit your assignment at the administrative counter.

2 Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).

3 Late submissions will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.

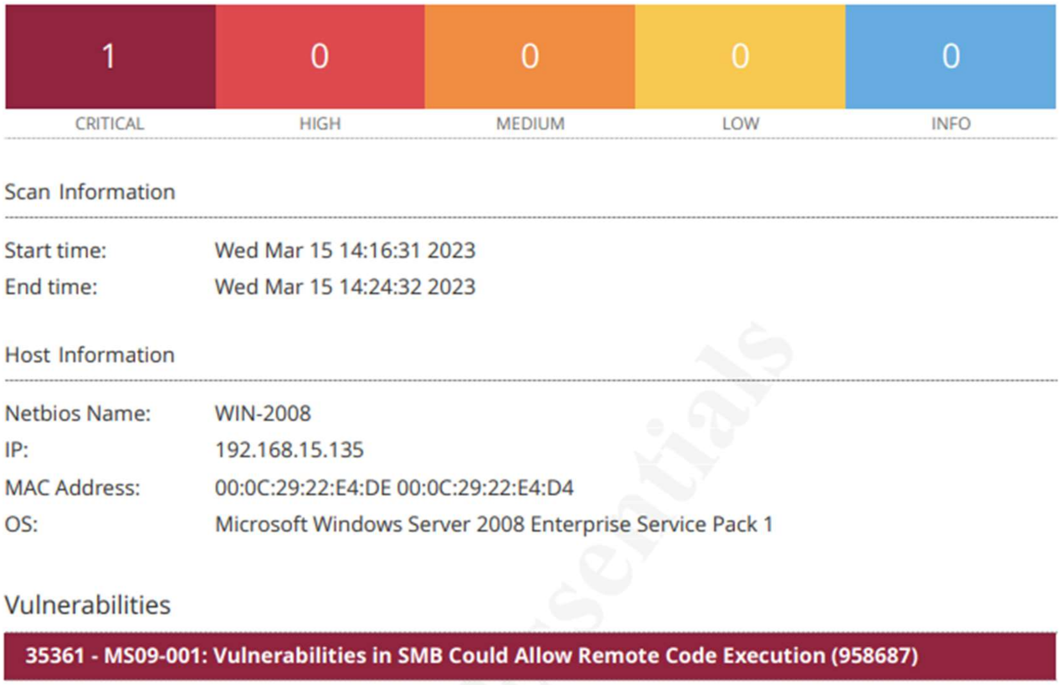
4 Cases of plagiarism will be penalized.

5 The assignment should be bound in an appropriate style (comb bound or stapled).

TABLE OF CONTENT

1.0 Summary from Section A

1.1 Critical Vulnerability: MS09-001 SMB Vulnerability Recap



1	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Mar 15 14:16:31 2023
End time:	Wed Mar 15 14:24:32 2023

Host Information

Netbios Name:	WIN-2008
IP:	192.168.15.135
MAC Address:	00:0C:29:22:E4:DE 00:0C:29:22:E4:D4
OS:	Microsoft Windows Server 2008 Enterprise Service Pack 1

Vulnerabilities

35361 - MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)

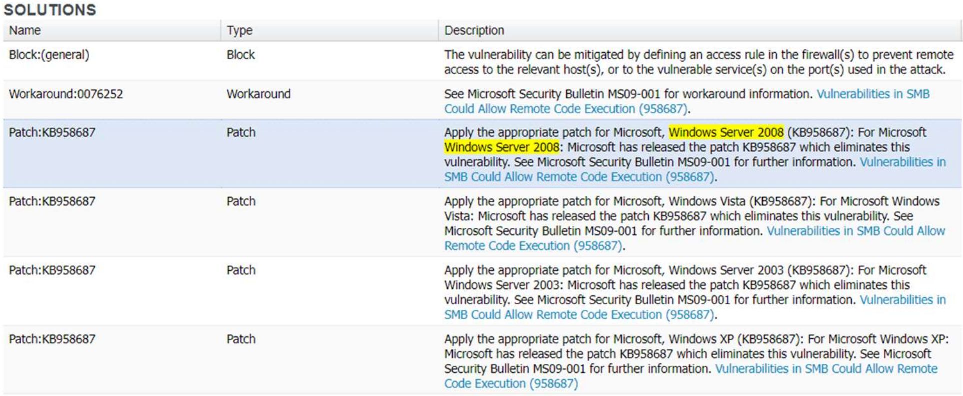
Figure 1 – *MS09-001: Vulnerability in SMB Could Allow Remote Code Execution (958687), Nessus*

As discussed in **Section A** of our Group 19 DSF Assignment, the vulnerability I have chosen is the **MS09-001 SMB Protocol** Vulnerability that was detected by Nessus as shown in Figure 1. This scan addresses a **critical** vulnerability that was found in the Windows 2008 Operating System in the **Server Message Block** (SMB) protocol sector (FortiGuard, 2010). In short, this vulnerability exists because of **human errors** concerning **memory management** of the operating system using **C / C++**. As a result, attackers can **send specially crafted packets** using **SMB** protocol to trigger a **buffer overflow** in the victims' computer, which will **overwrite data** into **adjacent** memory (shell) with their **own code**. As highlighted in Section A, **Conficker worm** (Ash-Dotan, 2016) had utilize this vulnerability to install **Keyloggers, Botnet Software, Fake Antivirus** and **Ransomware** onto the victims' computer, and **propagate** itself onto vulnerable computer **on the same network** through port 455 (Cobb, n.d.) in 2008, and resulted in **ten of billions** in damages.

2.0 Identify Patches and Solution

2.1 Identify Patch Needed

It is notable that this vulnerability, MS09-001 was **patched** in **2009** by Microsoft. Thus, the easiest way to protect the Windows 2008 virtual machine, is to **install the security update** that was released by Microsoft that year.



SOLUTIONS

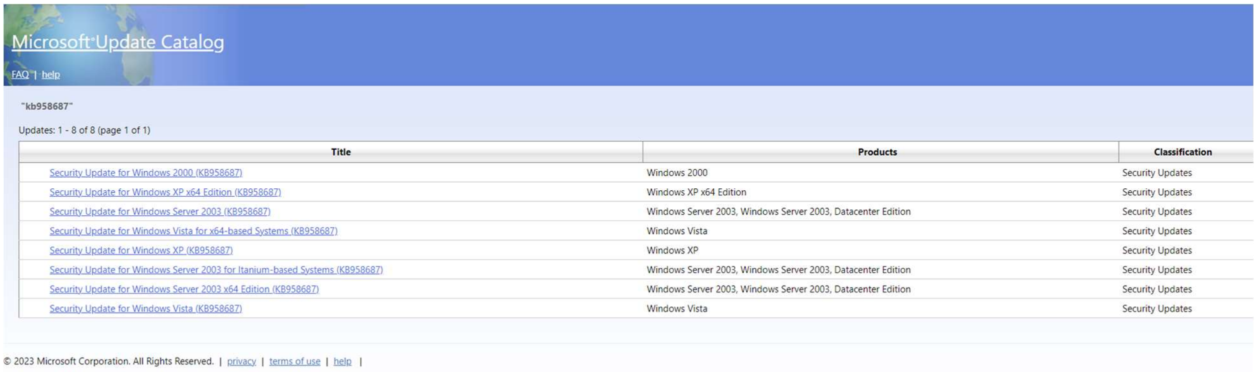
Name	Type	Description
Block:(general)	Block	The vulnerability can be mitigated by defining an access rule in the firewall(s) to prevent remote access to the relevant host(s), or to the vulnerable service(s) on the port(s) used in the attack.
Workaround:0076252	Workaround	See Microsoft Security Bulletin MS09-001 for workaround information. Vulnerabilities in SMB Could Allow Remote Code Execution (958687).
Patch:KB958687	Patch	Apply the appropriate patch for Microsoft, Windows Server 2008 (KB958687): For Microsoft Windows Server 2008: Microsoft has released the patch KB958687 which eliminates this vulnerability. See Microsoft Security Bulletin MS09-001 for further information. Vulnerabilities in SMB Could Allow Remote Code Execution (958687).
Patch:KB958687	Patch	Apply the appropriate patch for Microsoft, Windows Vista (KB958687): For Microsoft Windows Vista: Microsoft has released the patch KB958687 which eliminates this vulnerability. See Microsoft Security Bulletin MS09-001 for further information. Vulnerabilities in SMB Could Allow Remote Code Execution (958687).
Patch:KB958687	Patch	Apply the appropriate patch for Microsoft, Windows Server 2003 (KB958687): For Microsoft Windows Server 2003: Microsoft has released the patch KB958687 which eliminates this vulnerability. See Microsoft Security Bulletin MS09-001 for further information. Vulnerabilities in SMB Could Allow Remote Code Execution (958687).
Patch:KB958687	Patch	Apply the appropriate patch for Microsoft, Windows XP (KB958687): For Microsoft Windows XP: Microsoft has released the patch KB958687 which eliminates this vulnerability. See Microsoft Security Bulletin MS09-001 for further information. Vulnerabilities in SMB Could Allow Remote Code Execution (958687)

Figure 2 – *Solutions to Patch MS09-001, https://www.vulnerabilitycenter.com/#!vul=20492*

Figure 2 from (Security, 2019) shows that I need to look for **patch "KB958687"** which was designed to patch the MS09-001 vulnerability found on Windows Server 2008.

2.2 Patch Download Source

Next, I proceed to search the internet for patch "KB958687", which brought me to multiple legacy website that still contains the downloadable patch as detailed in Figure 3 below (Microsoft, 2009). Now that we have found the security patch, we shall begin with the technical steps to patch it.



"kb958687"

Updates: 1 - 8 of 8 (page 1 of 1)

Title	Products	Classification
Security Update for Windows 2000 (KB958687)	Windows 2000	Security Updates
Security Update for Windows XP x64 Edition (KB958687)	Windows XP x64 Edition	Security Updates
Security Update for Windows Server 2003 (KB958687)	Windows Server 2003, Windows Server 2003, Datacenter Edition	Security Updates
Security Update for Windows Vista for x64-based Systems (KB958687)	Windows Vista	Security Updates
Security Update for Windows XP (KB958687)	Windows XP	Security Updates
Security Update for Windows Server 2003 for Itanium-based Systems (KB958687)	Windows Server 2003, Windows Server 2003, Datacenter Edition	Security Updates
Security Update for Windows Server 2003 x64 Edition (KB958687)	Windows Server 2003, Windows Server 2003, Datacenter Edition	Security Updates
Security Update for Windows Vista (KB958687)	Windows Vista	Security Updates

© 2023 Microsoft Corporation. All Rights Reserved. | privacy | terms of use | help |

Figure 3 – *KB958687 Patch, https://www.catalog.update.microsoft.com/Search.aspx?q=kb958687*

3.0 Technical Steps

3.1 Step by Step Guide to Patch the Vulnerability

3.1.1 Step 1: Boot up your virtual machine.

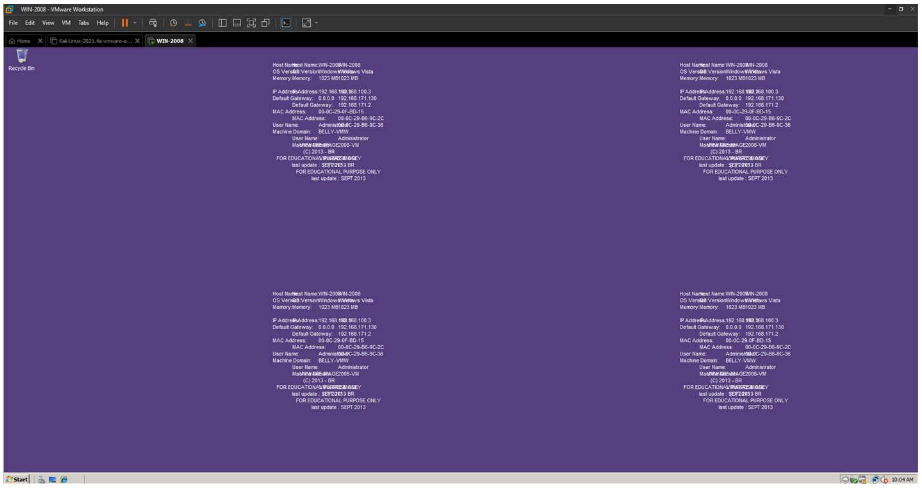
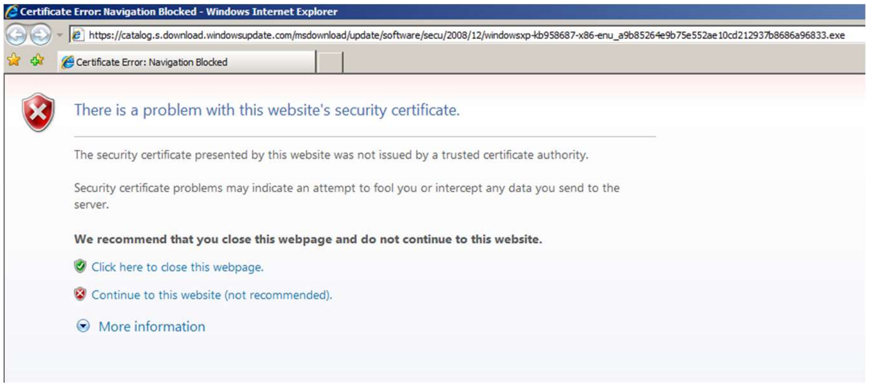


Figure 4 - *Windows 2008 VM*

Once we have logged into the virtual machine, we can now begin our technical surgery.

3.1.2 Open up the Patch Link on Internet Explorer


Certificate Error: Navigation Blocked - Windows Internet Explorer
Certificate Error: Navigation Blocked

https://catalog.s.download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

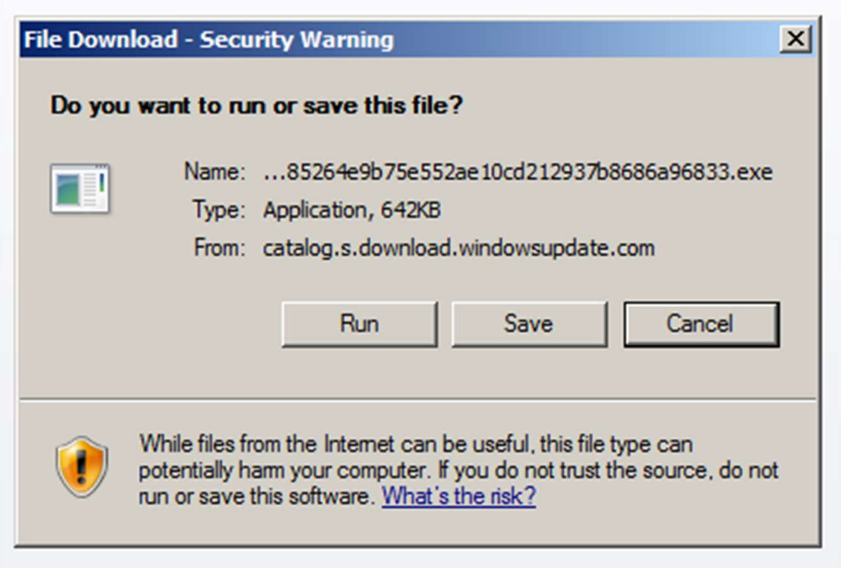
Continue to this website (not recommended).

More information

Figure 5 – *Navigate to Patch Download Link*

After arriving at the patch download page, click “**continue to this website**”.

3.1.3 Download the Patch


File Download - Security Warning

Do you want to run or save this file?

Name: ...85264e9b75e552ae10cd212937b8686a96833.exe

Type: Application, 642KB

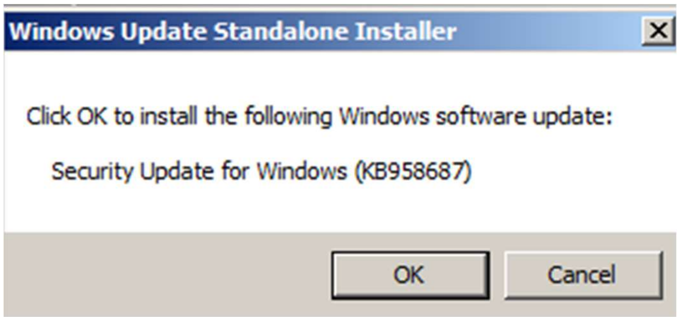
From: catalog.s.download.windowsupdate.com

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 6 – *File Download, Security Warning*

You should now see a pop-up to ask you if you want to "Run", "Save" or "Cancel" this patch. For my case, I clicked on "Save" to save it onto my local downloads folder first, and then click **run** after it was saved.

3.1.4 Install the Update


Windows Update Standalone Installer

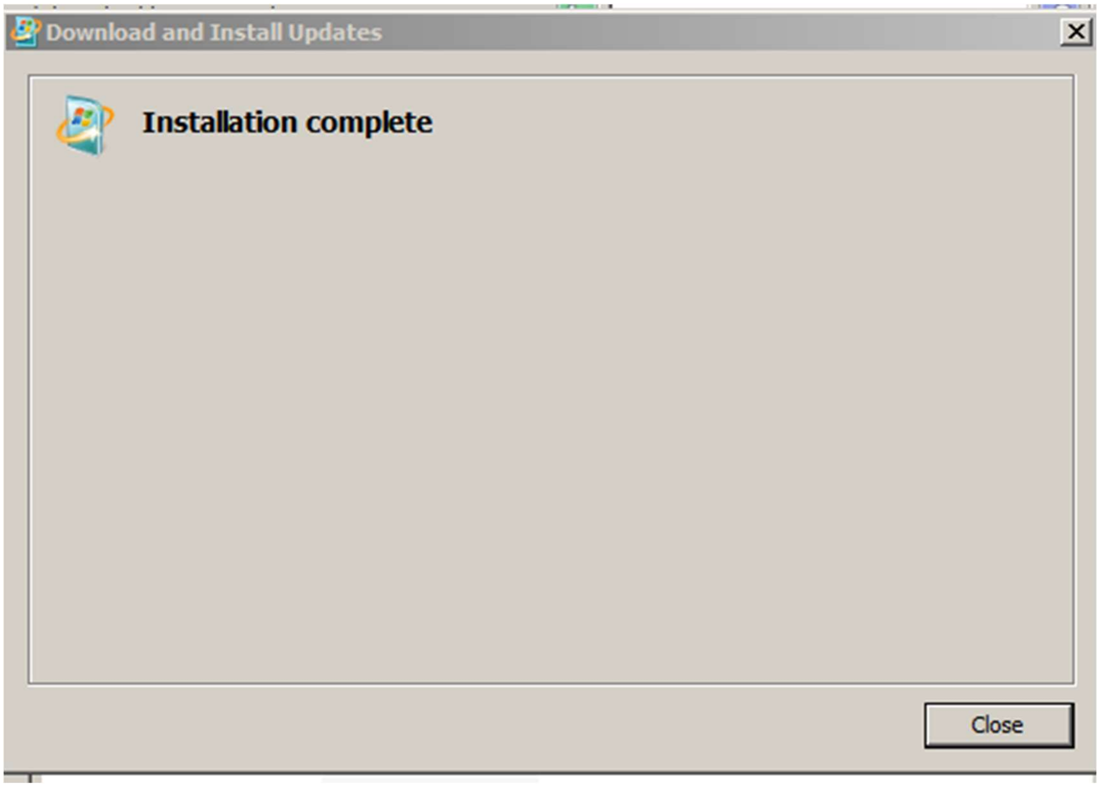
Click OK to install the following Windows software update:

Security Update for Windows (KB958687)

Figure 7 – *Windows Update Standalone Installer for patch KB958687*

After running the update patch, you will encounter Figure 7, which prompts if you want to install the KB958687 security update. Simply click **ok** to continue.

3.1.5 Installation Complete



Installation complete

Figure 8 - *Installation Complete*

Once its installed, a pop-up window will appear, signifying that the installation of security patch KB958687 was successful.

3.2 Steps to verify that this vulnerability has been removed.

3.2.1 Select Programs and Features in Control Panel

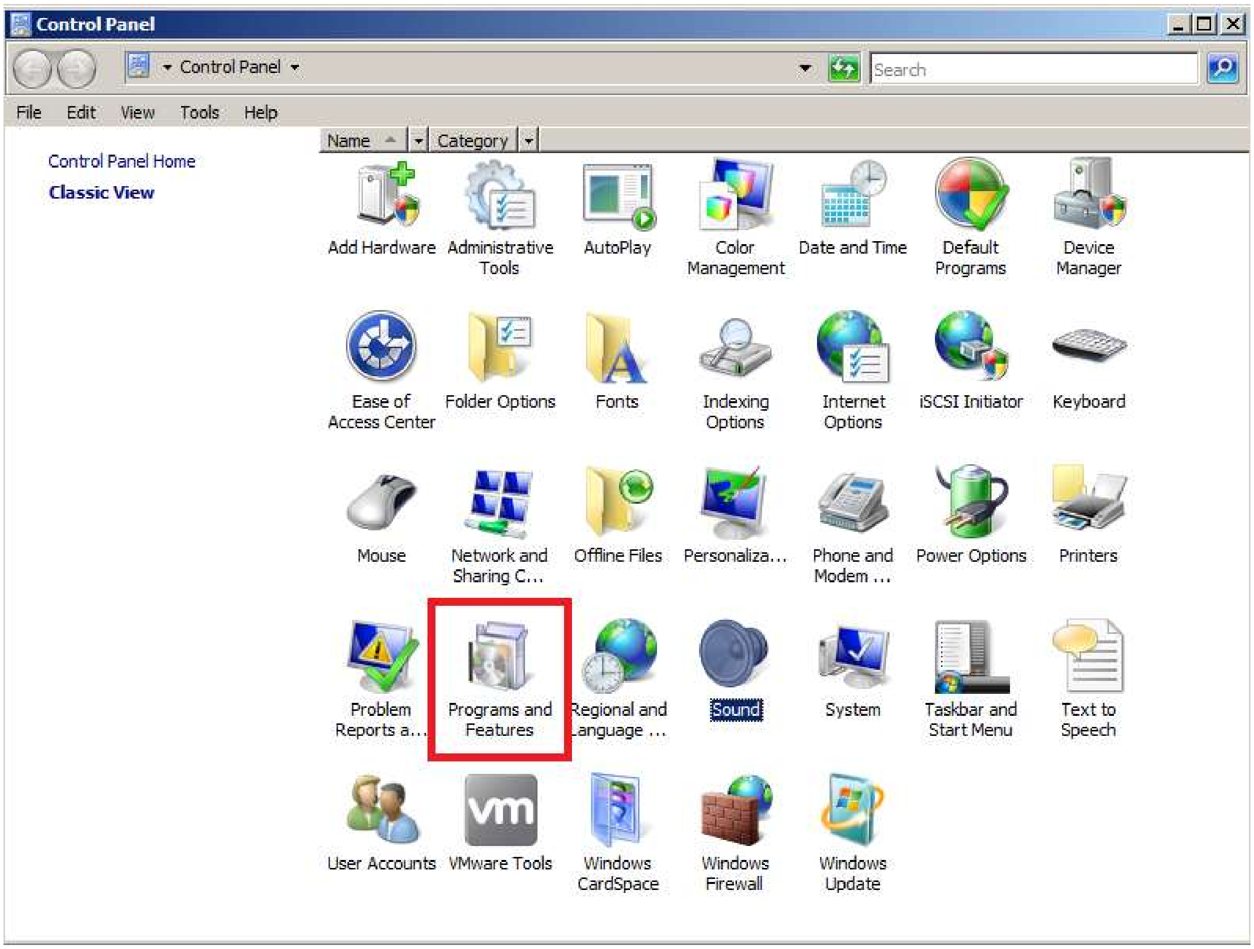
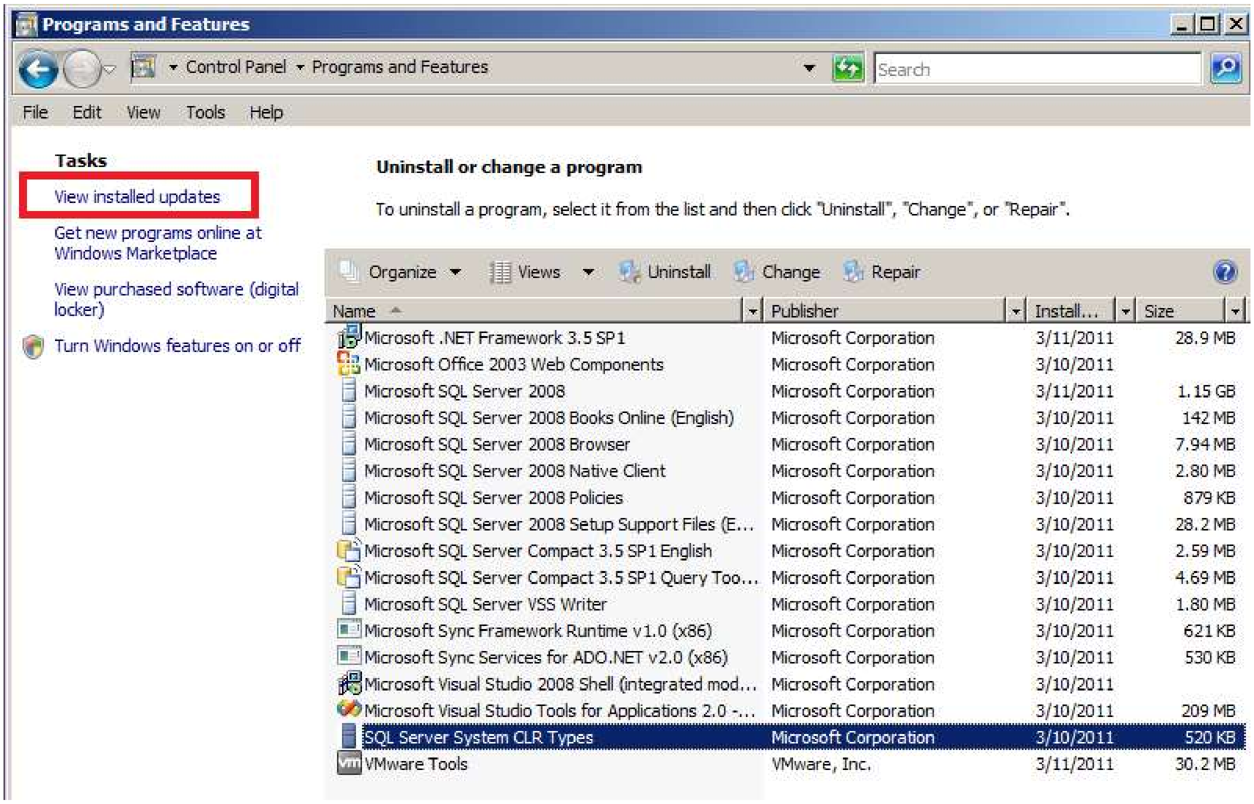


Figure 9 – *Programs and Features, Control Panel*

After installing the patch, I performed a quick check to verify whether the vulnerability MS09-001 has indeed been successfully patch. To do this, I selected "programs and features" in the control panel, as shown in Figure 9 above.

3.2.2 Click on “view installed updates”.


Programs and Features
Control Panel ▸ Programs and Features
Search
File Edit View Tools Help
Tasks
View installed updates
Get new programs online at Windows Marketplace
View purchased software (digital locker)
Turn Windows features on or off
Organize
Views
Uninstall
Change
Repair

Uninstall or change a program

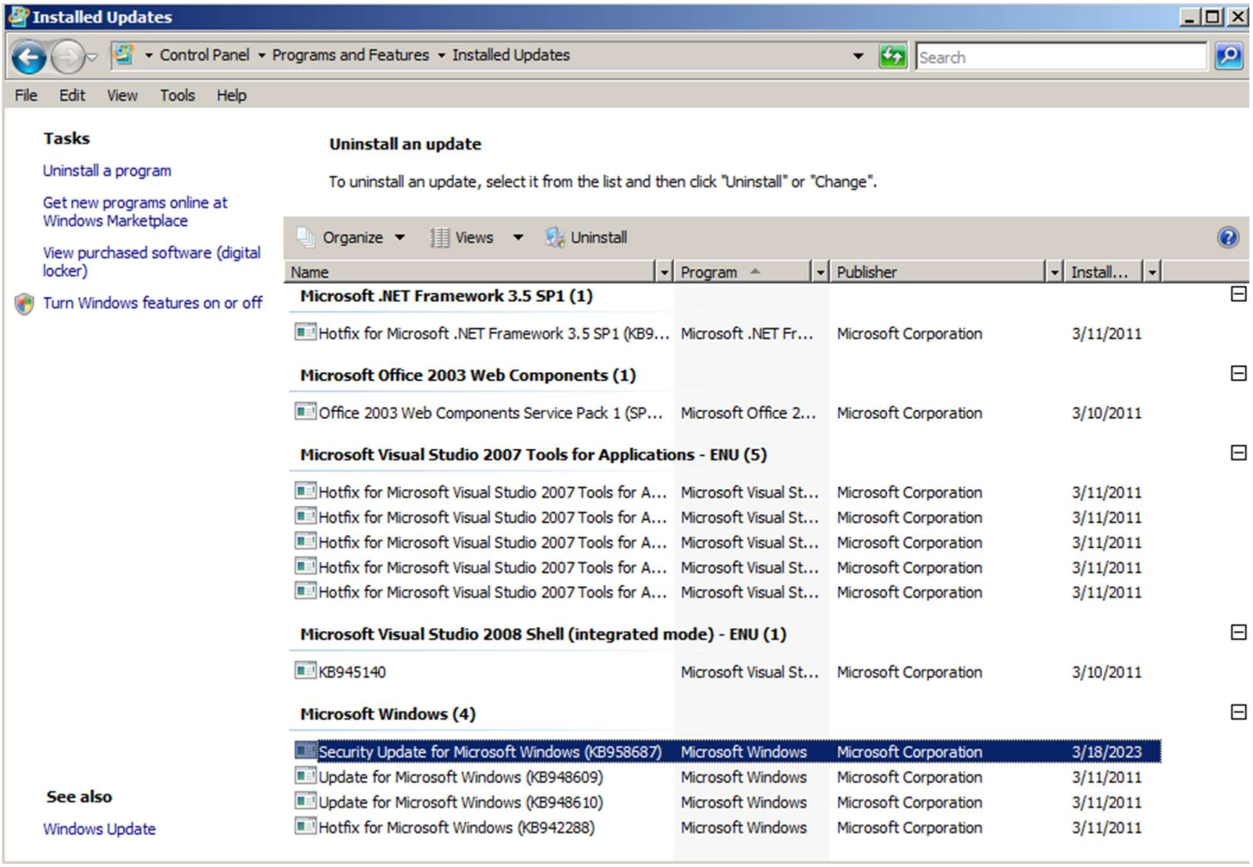
To uninstall a program, select it from the list and then click "Uninstall", "Change", or "Repair".

Name	Publisher	Install...	Size
Microsoft .NET Framework 3.5 SP1	Microsoft Corporation	3/11/2011	28.9 MB
Microsoft Office 2003 Web Components	Microsoft Corporation	3/10/2011	
Microsoft SQL Server 2008	Microsoft Corporation	3/11/2011	1.15 GB
Microsoft SQL Server 2008 Books Online (English)	Microsoft Corporation	3/10/2011	142 MB
Microsoft SQL Server 2008 Browser	Microsoft Corporation	3/10/2011	7.94 MB
Microsoft SQL Server 2008 Native Client	Microsoft Corporation	3/10/2011	2.80 MB
Microsoft SQL Server 2008 Policies	Microsoft Corporation	3/10/2011	879 KB
Microsoft SQL Server 2008 Setup Support Files (E...	Microsoft Corporation	3/10/2011	28.2 MB
Microsoft SQL Server Compact 3.5 SP1 English	Microsoft Corporation	3/10/2011	2.59 MB
Microsoft SQL Server Compact 3.5 SP1 Query Too...	Microsoft Corporation	3/10/2011	4.69 MB
Microsoft SQL Server VSS Writer	Microsoft Corporation	3/10/2011	1.80 MB
Microsoft Sync Framework Runtime v1.0 (x86)	Microsoft Corporation	3/10/2011	621 KB
Microsoft Sync Services for ADO.NET v2.0 (x86)	Microsoft Corporation	3/10/2011	530 KB
Microsoft Visual Studio 2008 Shell (integrated mod...	Microsoft Corporation	3/10/2011	
Microsoft Visual Studio Tools for Applications 2.0 -...	Microsoft Corporation	3/10/2011	209 MB
SQL Server System CLR Types	Microsoft Corporation	3/10/2011	520 KB
VMware Tools	VMware, Inc.	3/11/2011	30.2 MB

Figure 10 – *view installed updates, control panel*

Then, select “view installed updates” under the “Task” sidebar.

3.2.3 Check for the security patch.


Installed Updates
Control Panel ▸ Programs and Features ▸ Installed Updates
Search
File Edit View Tools Help
Tasks
Uninstall a program
Get new programs online at Windows Marketplace
View purchased software (digital locker)
Turn Windows features on or off
See also
Windows Update
Organize
Views
Uninstall

Uninstall an update

To uninstall an update, select it from the list and then click "Uninstall" or "Change".

Name	Program	Publisher	Install...
Microsoft .NET Framework 3.5 SP1 (1)			
Hotfix for Microsoft .NET Framework 3.5 SP1 (KB9...	Microsoft .NET Fr...	Microsoft Corporation	3/11/2011
Microsoft Office 2003 Web Components (1)			
Office 2003 Web Components Service Pack 1 (SP...	Microsoft Office 2...	Microsoft Corporation	3/10/2011
Microsoft Visual Studio 2007 Tools for Applications - ENU (5)			
Hotfix for Microsoft Visual Studio 2007 Tools for A...	Microsoft Visual St...	Microsoft Corporation	3/11/2011
Hotfix for Microsoft Visual Studio 2007 Tools for A...	Microsoft Visual St...	Microsoft Corporation	3/11/2011
Hotfix for Microsoft Visual Studio 2007 Tools for A...	Microsoft Visual St...	Microsoft Corporation	3/11/2011
Hotfix for Microsoft Visual Studio 2007 Tools for A...	Microsoft Visual St...	Microsoft Corporation	3/11/2011
Hotfix for Microsoft Visual Studio 2007 Tools for A...	Microsoft Visual St...	Microsoft Corporation	3/11/2011
Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (1)			
KB945140	Microsoft Visual St...	Microsoft Corporation	3/10/2011
Microsoft Windows (4)			
Security Update for Microsoft Windows (KB958687)	Microsoft Windows	Microsoft Corporation	3/18/2023
Update for Microsoft Windows (KB948609)	Microsoft Windows	Microsoft Corporation	3/11/2011
Update for Microsoft Windows (KB948610)	Microsoft Windows	Microsoft Corporation	3/11/2011
Hotfix for Microsoft Windows (KB942288)	Microsoft Windows	Microsoft Corporation	3/11/2011

Figure 11 - *Security Patch has been successfully installed, Control Panel*

This tab will display several patches that was once installed on this virtual machine. All I need to do, is to find the **KB958687** patch that I have just installed a few minutes ago. As you can see in Figure 11 above, I have **successfully** installed the update, and **patched** the MS09-001 SMB Vulnerability in the system, as **confirmed** by the Control Panel.

4.0 Conclusion

In conclusion, it is **important** to keep your security patches up to date regardless of the Operating System you are using. The process may be **cumbersome**, but it can **save the world ten of billions of dollars** in losses if it was done before the **Conficker** worm attack in 2008. As such, remember to always check for windows update, and install them, as it is easy, safe, and secure.

5.0 References

Ash-Dotan, L. (12 September, 2016). *What is the conficker worm?* Retrieved from Cybereason: https://www.cybereason.com/blog/what-is-the-conficker-worm

Cobb, M. (n.d.). *buffer overflow*. Retrieved from techtarget: https://www.techtarget.com/searchsecurity/definition/buffer-overflow

FortiGuard. (28 March, 2010). *Microsoft.SMB.Remote.Code.Execution.MS09.001*. Retrieved from FortiGuard Labs: https://www.fortiguard.com/encyclopedia/ips/20399/microsoft-smb-remote-code-execution-ms09-001

Microsoft. (13 January, 2009). *Security Patches for KB958687*. Retrieved from Microsoft Update Catalog: https://www.catalog.update.microsoft.com/Search.aspx?q=kb958687

Security, S. (14 7, 2019). *[MS09-001] Microsoft Windows SMB Protocol Buffer Overflow Remote DoS or Code Execution*. Retrieved from Skybox Security: https://www.vulnerabilitycenter.com/#!vul=20492

Author Details:

Name: Gan Ming Liang

Student ID: TP063338

Course: UCDF2104ICT(SE)

Thank you for reading.