Hello Everyone! In this exercise, you will learn about a Remote Desktop protocol-based vulnerability and its exploitation in Windows OS. BlueKeep is a software vulnerability affecting older versions of Microsoft Windows. Bluekeep Vulnerability only impacts Windows 7, Windows Server 2008 R2, and Windows Server 2008. Windows 8 and Windows 10 systems are not affected by this vulnerability.

Here are some news headlines and reports related to Blue Keep's vulnerability. Californian tech firm Vectra has revealed suspicious RDP behaviors in 90% of companies using RDP, with organizations in the manufacturing, finance and insurance, retail, government, and healthcare industries identified as being most at risk of attack.

So what is Remote Desktop protocol? It is a procedure used to operate a computer remotely using another device. It enables you to access a machine located elsewhere through a program and over the Internet. RDP is mainly used for file transfer, desktop sharing, application use, customer support, and troubleshooting. RDP was initially launched by Microsoft, but it is available for both Windows and Mac OS.

The process of remotely accessing a machine is very easy.

Copyrighted Content

First, you'll need to know the IP address of the PC running the Remote Desktop Protocol, that you want to connect to. Open the remote desktop connection app on your machine by typing mstsc in run command. The Remote Desktop connection will get open after this. Provide ip address of the remote machine and press enter. You will be able to connect to the remote machine, by providing valid credentials.

BlueKeep vulnerability also known as code name (CVE-2019-0708) was detected in the year 2019 in the Remote Desktop Protocol (RDP) used by Microsoft Windows OS. A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, also known as 'Remote Desktop Services Remote Code Execution Vulnerability'. This vulnerability is wormable it spread rapidly in a network. When the Attacker sends a specially crafted packet and set the value for the Channel ID to something the RDP service isn't expecting, this causes a memory corruption bug which results in a memory crash dump.

Copyrighted Content

You can check, whether your machine is vulnerable to RDP Blukeep attack, using a small utility called RDP scan. To do so, download the latest version of rdpscan from https://github.com/robertdavidgraham/rdpscan/releases

After download , Extract file of rdpscan-windows in default location.

Run the rdpscan utility from the command line as shown in figure.

Here you can see that a windows 7 machine is vulnerable to BlueKeep RDP vulnerability as rdpscan utility shows it as vulnerable.

If the attack happens on your machine, the following screen will be the first visible sign of an RDP blue keep attack. Attacker crashes kernel which cause a blue screen of death on victim machine. Due to RDP vulnerability on earlier version of windows, attacker can execute remote code execution and through backdoor victim machine get compromised. Attacker has full permission to remotely access victim machine, they can steal the important data, can execute malware encrypt files on the victim's machine and can misuse the stolen data for his benefits.

So, how would you respond if such attack happens on your machine? There are two activities that you can do to immediately handle such attack incidents. First Disable RDP service on your machine and then configure Network

Copyrighted Content

Level Authentication setting on your machine. Let's see how to do it.

Now when you have understood the Bluekeep attack, lets discuss, some protection techniques. There are many ways to protect yourself from such types of attacks. Disabling RDP service through firewall is one of them RDP service runs on port number 3389, which is used by the attacker to perform the attack. If RDP service is not required, it may be disabled by blocking the port number 3389 through the firewall. To block this service first ensure that the service is running using following steps.

Press Windows + R key combo to start the Run box.

Type "cmd" to start Command Prompt.
Type: "netstat –na" and press Enter.
netstat –na command scans and displays all connected ports.

In the given screenshot , you can find an entry with port no 3389 with listening state, which indicates that the service is running on the machine.

To disable the RDP service block the port number 3389. to do so, Go to Start , click on Control Panel click on Windows Firewall and find Advanced settings on the left side.

Copyrighted Content

Click on Inbound Rules > New rule. Then in the pop-up window, choose Port > Next >TCP > Specific local ports ,type 3389 in the text box and go to Next.

Choose Block the connection and click on Next.

Tick the three checkboxes and click Next.

Specify the name and description and click Finish.

To ensure that the rule is created, you can find the rule created in the inbound rules section.

Thank You!

Copyrighted Content